Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para la Empresa Javesalud I.P.S.

Javier Alexander Joya Cruz

Carlos Serjeif Sacristán Hernandez

Dirigido por:

PhD. Alexandra Maria López Sevillano

Diciembre 2017

Universidad Católica De Colombia

Facultad de Ingeniería

Especialización en Seguridad de la Información

Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para la Empresa Javesalud I.P.S.

Javier Alexander Joya Cruz

Carlos Serjeif Sacristán Hernandez

Universidad Católica De Colombia

Notas de Autor:

Carlos Serjeif Sacristán Hernandez, Especialización en Seguridad de la Información
Javier Alexander Joya Cruz, Especialización en Seguridad de la Información
Este proyecto ha sido parcialmente financiado por JAVESALUD I.P.S.
La correspondencia relacionada debe ser dirigida a Javier Joya y Carlos Sacristán
Facultad de Ingeniería, Universidad Católica de Colombia, Bogotá, Diagonal 46 A # 15 B – 10
Contatos: jajoya49@ucatolica.edu.co, cssacristan59@ucatolica.edu.co

TABLA DE CONTENIDO

Lista de Tablas

Lista de Ilustraciones

Resumen

En la actualidad, el sector de salud ha avanzado en el ámbito tecnológico, incorporando nuevos procesos informáticos a partir del uso de las TIC (Tecnologías de la información y las comunicaciones) con el fin de mejorar la calidad del servicio, ofreciendo eficacia y eficiencia al momento de recopilar datos, generar nueva información de clientes, garantizar disponibilidad de dicha información a roles específicos y así asegurar la confidencialidad de la información.

Las empresas entienden que los activos de información son relevantes para definir la correcta implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), que permita identificar amenazas y vulnerabilidades de los activos más esenciales y así crear controles a los riesgos críticos que amenacen la continuidad del negocio.

El proyecto brinda un análisis de los activos lógicos de información de la empresa Javesalud, con el fin de encontrar los posibles riesgos y amenazas a los que se encuentran expuestos.

Por medio de la metodología Magerit v.3, cada activo lógico es clasificado en una matriz de acuerdo con su interrelación el valor que posee, identificando que depreciación o coste generaría en la organización. Proyecta un descubrimiento de riesgos a raíz de eventos adversos encontrados para cada activo enlistado. Posteriormente se realiza una matriz de priorización de riesgos donde el objetivo principal es evaluar el impacto que genera cada riesgo encontrado, clasificando su causa y probabilidad de reproducción. Finalmente se crean controles a partir de los riesgos encontrados se elabora un documento relacionando la forma de implementación de dichos controles y buenas prácticas de gestión de sistemas informáticos para que la organización lo utilice.

PALABRAS CLAVE: Tecnologías de la información y las comunicaciones (TIC’s), Sistema de Gestión de Seguridad de la información (SGSI), Activos de información, Vulnerabilidades, Amenazas, Riesgos, Controles, Metodología Magerit v.3.

Abstract

Currently, the health sector has advanced in the technological field, incorporating new computer processes from the use of ICT (Information and Communication Technologies) in order to improve the quality of service, offering efficiency and effectiveness to the time to collect data, generate new customer information, ensure availability of such information to specific roles and thus ensure the confidentiality of information.

The companies understand that the information assets are relevant to define the correct implementation of an Information Security Management System (ISMS), which allows to identify threats and vulnerabilities of the most essential assets and thus create controls to the critical risks that threaten the continuity of the business.

The project provides an analysis of the logical information assets of the Javesalud company, in order to find the possible risks and threats to which they are exposed.

By means of the Magerit v.3 methodology, each logical asset is classified in a matrix according to its interrelation the value it has, identifying what depreciation or cost would generate in the organization. Project a risk discovery due to adverse events found for each asset listed. Subsequently, a risk prioritization matrix is carried out where the main objective is to evaluate the impact generated by each risk found, classifying its cause and probability of reproduction. Finally, controls are created based on the risks found. A document is elaborated relating the way of implementation of said controls and good practices of computer systems management for the organization to use it.

KEYWORDS: Information and communication technologies (ICTs), Information Security Management System (ISMS), Information assets, Vulnerabilities, Threats, Risks, Controls, Magerit Methodology v.3

Introducción

En el proceso de recopilación de datos e información, el ser humano ha buscado desde tiempos antiguos por medio de la práctica y la experiencia la forma de aprender y organizar ideas para facilitar su fácil acceso.

En el transcurso del tiempo se ha vuelto indispensable mantener, controlar y organizar la información que se ha obtenido por medio del aprendizaje, lo cual ha adquirido gran valor en la actualidad. Los sistemas de información son uno de los activos más valiosos para una empresa o entidad, los datos que almacena y su manipulación para el progreso y logro de los objetivos y metas que ha planteado la entidad.

El avance tecnológico ha generado nuevos procesos de manipulación de los activos de información en la parte lógica, estipulando controles en equipos de cómputo, medios de trasmisión, dispositivos de almacenamientos con el fin de facilitar nuevas posibilidades de acceso a los usuarios. Lo anterior crea el estigma de que “los sistemas de información no son totalmente seguros”, hipótesis tomada a partir del análisis realizado a los eventos adversos presentados en los historiales de otras compañías como “HBGARY”, donde se evidencian intrusiones a sistemas por agentes externos, identificando falencias en los accesos y así estipulando la pérdida del activo. Por esta razón es necesario garantizar la seguridad de la información de forma continua, dando confiabilidad, confidencialidad, integridad y disponibilidad a la base de información con la que cuentan las entidades.

En ese ámbito las entidades de salud han realizado un avance bastante significativo en la utilización de procesos informáticos, sin embargo, los diferentes riesgos, vulnerabilidades o amenazas de este tipo de procesos pasan desapercibidos por estas entidades, lo cual se convierte en un tema de suma importancia, teniendo presente que la legislación nacional e internacional, como la Resolución

número 1995 de 1999…. del ministerio de salud o la LEX ARTIS o Ley del arte para profesionales de la salud, referida a la Ley 23 de 1981 y al Decreto 3380 de 1981, que habla sobre la confidencialidad de la información de los pacientes, así como la moral profesional de los empleados que brindan el servicio, relacionando como responsables de la información sensible a las entidades de salud siendo de carácter prioritario su custodia y manejo.

La empresa Javesalud IPS es una organización comprometida con sus pacientes, por lo que se hace necesario gestionar un sistema de protección de la información de los pacientes y los procesos documentados digitalmente, con el fin de asegurar la información de los clientes internos y externos, evitando que un ente no deseado pueda realizar modificaciones a los activos de información, poniendo en riesgo la confiabilidad y disponibilidad de los datos.

En este proyecto se pretende generar la propuesta de un plan de mitigación de riesgos y vulnerabilidades, iniciando con una evaluación de los activos lógicos de información que posee la empresa para determinar aquellos que pueden generar un mayor impacto en la entidad, de la mano con la aplicación de nuevas políticas de seguridad informática que permitan contribuir al desarrollo de un Sistema de gestión de la Información (SGSI) dentro de la entidad para el mejoramiento continuo del control y acceso del activo.

1. Generalidades

1.1. Línea de Investigación

La línea de investigación está sustentada en GISIC (Software Inteligente y Convergencia Tecnológica) debido a que el proyecto comprende políticas, gestión y métodos de innovación para la seguridad de la información de la entidad; además la seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo)

1.2. Alcance del proyecto

Este proyecto abarca el desarrollo de una propuesta de controles para la mitigación de riesgos y vulnerabilidades, para JAVESALUD IPS, esto con el propósito de mejorar la confidencialidad, disponibilidad e integridad de la información manejada y procesada en la empresa.

Para desarrollar la propuesta, se aplicarán herramientas concernientes a los modelos de análisis y evaluación de riesgos que permitan detectar las vulnerabilidades existentes en la seguridad de los activos lógicos de la entidad; como parte de este diagnóstico se pretende evaluar la infraestructura, los roles con autorización de ingreso a información sensible, y las políticas de seguridad de la información estipuladas en la empresa.

El proyecto generara un informe de controles, y no su implementación ya que se deja con completa autonomía a la alta gerencia de la entidad el adoptar o no los controles propuestos.

1.3. Planteamiento del Problema

En la actualidad, gran parte de las instituciones del sector salud del país se apoyan en las tecnologías de la información y las comunicaciones para realizar los procesos más importantes de sus labores diarias. A medida que el manejo de la información es más complejo, los centros de salud tienen el deber de implementar sistemas de gestión de seguridad, que eviten la ejecución de procesos innecesarios, erróneos o que afecten la calidad del servicio.

La información se ha convertido en el activo más importante de la mayoría de las instituciones y por lo tanto se deben implementar controles de seguridad física y lógica que permitan asegurar la información, aplicando protección en sus actividades logrando la optimización de los servicios administrativos.

Desde este punto de vista mediante una verificación en la documentación registrada en los sistemas de información, áreas de calidad y área de tecnología en la entidad JAVESALUD IPS, se logró determinar que en sus procesos informáticos no cuenta con un estudio vigente acerca de los posibles riesgos y vulnerabilidades que pueda presentar, por tal motivo es necesario realizar un análisis y revisión que permita tomar medidas de control para minimizar los riesgos inminentes que puedan afectar el sistema de información de la institución.

1.3.1. Antecedentes.

En marzo de 2014, la base de datos contenida en 27 DVD de pacientes pertenecientes al sistema de salud NHS del Reino Unido fue entregada a la gestión de un grupo de consultores, quienes subieron la información a servidores de Google fuera del Reino Unido. Las consecuencias de esto se resumen en cuatro situaciones delicadas: 1. La policía tuvo acceso por la "puerta trasera" a los historiales médicos de pacientes ambulatorios y hospitalizados. 2. Se utilizaron los datos para localización de los pacientes por parte de terceros. 3. Organizaciones como laboratorios farmacéuticos, compañías aseguradoras y proveedores de salud privados adquirieron los registros médicos de los pacientes desde el año 1999. 4. La información extraída contenía: número NHS de la persona, fecha de nacimiento, código postal, etnia y género. Los grupos de pacientes se preguntaron: ¿qué garantías existen para proteger la privacidad de la información médica? (Karim Nader Ch. (abril 2016), Riesgos en la seguridad informática en la salud)

Websense es una empresa que se especializa en proteger las empresas en cuanto a ciberataques,

y genera un informe de los sectores más atacados, en el 2015 el informe presento un 340% más incidentes de seguridad en el sector salud que en las otras industrias, así como un 74% más probabilidad de sufrir impacto por los esquemas de phishing, 4.5 veces más el impacto de un criptowall y 3 veces más de probabilidades de ser afectada por Dyre. (Luciana Zazzali (noviembre 2015), Seguridad informática en el sector salud. Recuperado de http://distribucion.itsitio.com/ar/seguridad-informatica-en-el-sector-salud).

Según la Oficina de Derechos Civiles de EE. UU., en 2015 se produjeron unos 253 agujeros de seguridad informática en el sector sanitario que afectaron a más de 500 personas con el robo de más de 112 millones de registros. IBM asegura por su parte que fue la industria más atacada. (Martínez Ana, (agosto 2016), Millones de datos de pacientes, en riesgo por los agujeros de seguridad informática. Recuperado de http://www.abc.es/tecnologia/redes/abci-millones-datos-pacientes-riesgo-agujeros-seguridad-informatica-201608070100_noticia.html.

En 2015, se filtraron los datos de 11 millones de clientes de la aseguradora Premera a raíz de un ataque de malware. Los códigos maliciosos y los ataques dirigidos no son los únicos riesgos que enfrenta la industria de la salud, ya que empleados (actuales o antiguos) también pueden causar incidentes de seguridad. (Dergarabedian Agustina, (enero 2016), Riesgos de seguridad informática en la industria de la salud. Recuperado de https://portinos.com/29333/riesgos-de-seguridad-informatica-en-la-industria-de-salud).

Según el avance y el alcance de las nuevas tecnologías, Javesalud IPS puede estar expuesta a amenazas en la seguridad de la información, robo, perdida de datos y ataques informáticos, lo que obliga a generar un análisis de riesgos además Las instituciones de salud como hospitales, clínicas y laboratorios se han convertido en un blanco atractivo para los cibercriminales, porque manejan información personal, financiera y médica de sus pacientes y personal. En estos ataques

entra en juego información básica junto con las dependencias a medicamentos, las necesidades de determinados tratamientos o prácticas especializadas y otros componentes que hacen a las personas.

1.4. Pregunta de investigación

¿La propuesta de mitigación de riesgos y vulnerabilidades de activos lógicos genera un impacto positivo en la protección de activos en Javesalud IPS?

1.5. Variables de investigación

1.5.1. Variable Independiente

La variable independiente es la causa principal del objeto de estudio y o el fenómeno estudiado, es aquella que puede ser manipulada por tanto la definición de la variable independiente es: "Propuesta de mitigación de riesgos y vulnerabilidades" como nuestra variable independiente.

1.5.2. Variable Dependiente

La variable dependiente, es la que se ve afectada por nuestra variable independiente, y que nos traerá mediciones que nos permitirán evaluar el objeto de estudio, en ese orden de ideas, la variable dependiente definida es "protección de activos y procesos críticos de la entidad"

1.5.3. Variable Interviniente

Las variables intervinientes, son características que afectan las variables dependientes, e independientes, y que al no controlarse puede generar una distorsión de los resultados de la investigación, para nuestro caso, la variable manejada es la política de seguridad actual en la entidad.

1.6. Justificación

Con este trabajo de investigación se pretende suplir un vacío en el proceso de seguridad informática en la entidad JAVESALUD IPS, incorporando una propuesta de controles para

mitigar riesgos y vulnerabilidades de sus activos lógicos.

Lo anterior en cuanto a que a partir de una validación de documentación de la entidad se encontró que no se ha desarrollado una evaluación de riesgos de estos activos, además que al generar esta propuesta se generara una necesidad social sobre los pacientes al garantizar de manera más efectiva la protección de su información clínica y datos personales.

El objetivo de este proyecto es crear una conciencia colectiva sobre la seguridad informática en todos los involucrados de la entidad, y que pueda generar una práctica continua para todos.

El proyecto va encaminado a realizar el inventario, la clasificación y la generación de controles de mitigación de riesgos de todos los activos lógicos de la entidad.

Conforme a lo anterior es de igual importancia la conveniencia que trae el proyecto a la normatividad actual sobre información asistencial sistematizada, sus beneficios económicos a mediano y largo plazo, y la mejora sustancial en el concepto de seguridad informática manejado por JAVESALUD IPS.

1.7. Objetivos

1.7.1. Objetivo general

- Realizar un análisis de riesgos a los activos lógicos de JAVESALUD IPS, aplicando el modelo MAGERIT 3.0 para generar un informe de controles, normativas y buenas prácticas enfocado a minimizar la probabilidad, la ocurrencia y el impacto de los riesgos más críticos.

1.7.2. Objetivos específicos

- Analizar los diferentes datos de la entidad para identificar los activos lógicos y su impacto en JAVESALUD.

- Desarrollar un análisis de riesgos y vulnerabilidades de la entidad JAVESALUD basado en el modelo MAGERIT 3.0 para medir el impacto y criticidad.
- Evaluar los riesgos más críticos según el modelo realizado para construir el informe de controles.
- Diseñar un plan de capacitación en cuanto a políticas de seguridad informática con el fin de incrementar los conocimientos de los colaboradores de la entidad.

2. Marcos de referencia

2.1. Marco conceptual

En el marco de la salud ya es necesario el manejo de la tecnología como herramienta a la prestación de servicios, por lo cual el manejo de términos informáticos cada vez es más frecuente. Los términos más utilizados en el trascurso del proyecto serán aquellos pertenecientes a la triada de la seguridad informático.

Confidencialidad: Acceso a los diferentes activos, dependiendo un rol establecido

Integridad: Modificación y creación de los diferentes activos, dependiendo un rol establecido

Disponibilidad: Cuando los usuarios requieran algún activo este debe estar disponible según el rol establecido.

Estándares de seguridad: "Si bien los estándares nos proporcionan una base importante para llegar a crear un modelo de seguridad, ésta se basa en las políticas de seguridad de la organización, las cuales determinan los procedimientos, los estándares y las herramientas que ayudarán a estas labores" (Gómez, J., diciembre 2013).

Historia clínica electrónica: Es una recopilación computarizada de los detalles de salud de un paciente. Pero es más que eso, es una nueva manera de almacenar y organizar la información del paciente. Al igual que las fichas de hospital, los archivos de EHR de los pacientes se dividen en secciones donde los profesionales en entran la información para proporcionarle cuidado médico al paciente o realizar tareas administrativas. (Michael, septiembre 2011).

Amenaza, Riesgo y Vulnerabilidad: En el ámbito de la ciberseguridad, podemos definir el riesgo como la probabilidad de que ocurra un incidente de seguridad. Como el riesgo no es más que una probabilidad, se puede medir y se suele cuantificar con un número entre 0 y 1 o con un porcentaje. Por otro lado, la amenaza es una acción que podría tener un potencial efecto negativo

sobre un activo. Es decir, una amenaza es cualquier cosa que pueda salir mal. Hay que tener en cuenta que una amenaza por sí misma no provoca un daño, pero podría provocarlo. Las amenazas se comprenden mejor si se clasifican atendiendo a cómo pueden dañar a un activo: esencialmente, pueden afectar a su disponibilidad, a su confidencialidad o su integridad (también pueden saltarse el control de acceso).

Para que se produzca un daño es necesario que exista una debilidad o fallo en el sistema que permita que se materialice una amenaza. Estas debilidades, fallos o "agujeros de seguridad" son las vulnerabilidades, que pueden ser de diferente naturaleza, de diseño, de arquitectura y configuración, de estándares de uso y procedimientos, etc. Es decir, cuando se dice que un activo es vulnerable, significa que tiene un agujero que puede ser aprovechado para provocar un incidente de seguridad. (Beltrán, mayo 2017).

Sistema de información: sistema de información es un conjunto de componentes que interaccionan entre sí para alcanzar un fin determinado, el cual es satisfacer las necesidades de información de dicha organización

Paciente: El paciente designa a un individuo que es examinado medicamente o al que se administra un tratamiento. Proviene del verbo latino "pati", que quiere decir "el que sufre": el paciente es, pues, una persona que es curada. El término paciente se puede declinar de varias maneras. Se le llama "sujeto" en las investigaciones. Los anglosajones hablan más a menudo de "clientes". Una nueva terminología está tomando importancia progresivamente: "actiente". (Pillou, noviembre 2013).

Auditoria Médica: La auditoría médica es un proceso interdisciplinario, que permite al Cuerpo Médico realizar la evaluación del acto médico, con los objetivos de mejorar la práctica médica, ser un medio de educación continua y mejorar la calidad de la atención médica. (Garaycochea,

marzo 2003).

Consulta Médica: Es la atención otorgada por un profesional de la salud a un paciente en su Consultorio Privado o en un box de atención destinado para estos efectos en un Hospital, Consultorio, Clínica o Centro de Salud, entre otros, que tiene como fin determinar un diagnóstico, realizar un control o tratamiento a seguir para una afección, enfermedad o problema de salud que afecta a un paciente, constituyendo la causa que motiva el acercamiento de las personas. (Fonasa, enero 2017).

Servidor de Dominio: El Servicio de Directorio Activo proporciona la capacidad de establecer un único inicio de sesión y un repositorio central de información para toda su infraestructura, lo que simplifica ampliamente la administración de usuarios y equipos, proporcionando además la obtención de un acceso mejorado a los recursos en red. Es un servicio de directorio, en el cual se puede resolver nombres de URLs o de determinados recursos. (Intef, enero 2017).

Roles: Un rol es una característica que permite agrupar los derechos de acceso a los recursos y asignarlos eficazmente a los usuarios. (ORACLE, enero 2010).

2.2. Marco teórico

2.2.1. Seguridad de la Información.

En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección. (Erb, agosto 2009).

2.2.2. Auditoria de información

Comprende una serie de tareas y procesos para determinar la situación de los activos de una

entidad, que buscan la eficiencia corporativa.

Conforme el proceso de auditoría indaga y cuestiona o valora cada dato en un proceso organizacional va profundizando su conocimiento en la gestión de los negocios importantes de la organización y a su vez es capaz de plantear objetivos de control que tratarán de proteger la información en su totalidad o parcialmente de acuerdo con las funciones organizacionales y a la definición de límites de acuerdo con los niveles de criticidad de la información identificados por cada organización.

2.2.3. Mitigación De Riesgos

Metodología para minimizar riesgos. Se fundamenta en prevalecer, valorar y efectuar los controles adecuados de reducción de riesgos sugeridos por el tratamiento de estimación del riesgo. Opciones de resolución para mitigar el riesgo:

- Aceptar el riesgo. Admitir el riesgo latente y seguir trabajando, o establecer controles para aminorar el riesgo a un estado admisible.
- Prevenir el riesgo. Suprimir el origen y/o secuela del riesgo.
- Disminuir el riesgo: Restringir el riesgo con el establecimiento de controles que disminuyen el efecto perjudicial de una amenaza que aprovecha una debilidad.

Opciones de tratamiento del riesgo: mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Disminuir la desvalorización ocasionada por una amenaza.
- Aminorar la posibilidad de que una amenaza se realice.

En los casos anteriores se debe aumentar u optimizar el grupo de protecciones.

Proteger los recursos de los sistemas de información de INGELEC S.A.S y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, con el fin de asegurar el

cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. (Citel, septiembre 2009).

2.2.4. Magerit.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. (Portal de Administración Electrónica Ministerio de Hacienda, España, 2017)

2.3. Marco contextual

Es una entidad prestadora de servicios de Salud. Dentro del portafolio de servicios que ofrece la fundación se encuentran consultas de medicina general, salud ocupacional, medicina familiar, urología, ortopedia, cirugía general, cirugía plástica, pediatría, ginecología - obstetricia, otorrinolaringología, cardiología, neumología. Con una atención centrada en el individuo bajo los

principios de medicina familiar prestando atención a pacientes que se encuentran afiliados a las EPS con las que se tienen vínculos contractuales, pacientes particulares y pacientes de zonas de influencia de las sedes de responsabilidad social dentro de la capacidad propia de cada sede.

Ilustración 1 *Mapa de Unidades Funcionales Javesalud IPS*

Misión y visión

Nuestra misión es "Prestar servicios de salud en el marco del cuidado primario, con dignidad humana, resolviendo con efectividad las necesidades de las personas. Generamos conocimiento en alianza con la academia y actuamos en un ambiente donde priman el respeto, la ética y la innovación".

Como aspectos más relevantes de la Misión se destaca:

El concepto de cuidado primario: que abarca las intervenciones ambulatorias más efectivas en el impacto de resolutividad a los principales motivos de consulta de la población y están en la puerta de entrada al sistema de salud. Bajo esta definición, la Fundación ofrece su portafolio de servicios ambulatorios de baja y mediana complejidad.

Dignidad Humana, como uno de los valores organizacionales.

Generación de conocimiento y alianza con la academia como uno de los pilares y el objeto final de la Fundación.

Respeto, Ética e Innovación, nuestros principios organizacionales.

Nuestra visión "En el 2016 Javesalud será una red integral e integrada de servicios de salud de cuidado primario, acreditada y reconocida por la gestión y prestación de servicios de salud, por fomentar la investigación y apoyar a la academia"

Resaltando los siguientes aspectos:

Red Integral e Integrada: Trabajo conjunto, articulado y estandarizado entre sus sedes, servicios y organizaciones de mayor nivel de complejidad buscando ofrecerle al usuario integralidad y continuidad en su atención.

Acreditada: Ofreciendo servicios de calidad superior como principio básico de la Fundación.

Fomentar la investigación y la academia: como objeto principal de la Fundación.

Organigrama de JAVESALUD

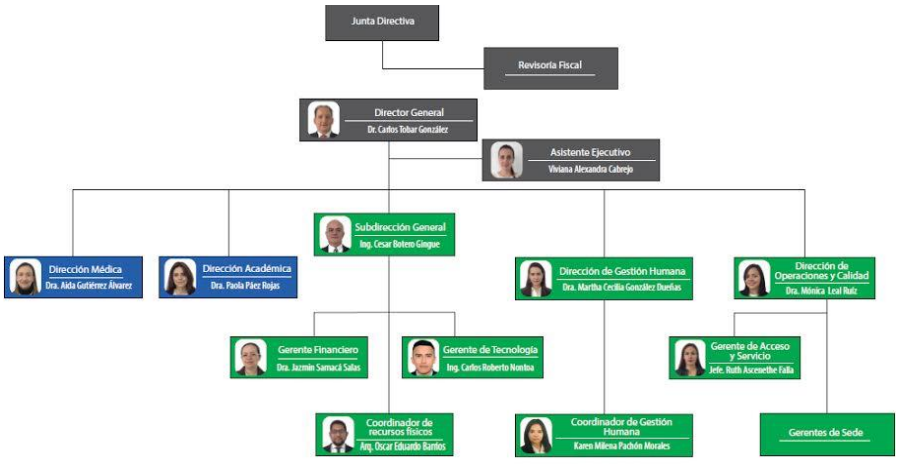


Ilustración 2 *Organigrama Javesalud IPS*

Organigrama de gerencia de tecnología e información.

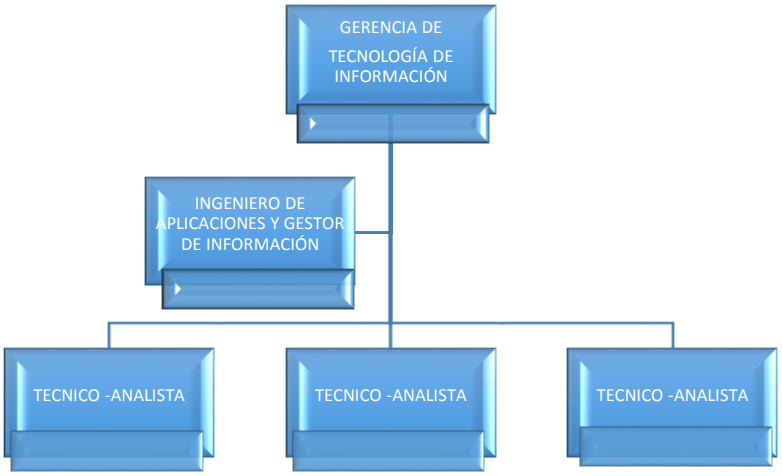


Ilustración 3 *Organigrama Tecnología de Información Javesalud IPS*

2.4. Marco Jurídico

Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales, y tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.", (http://www.suin-juriscol.gov.co)

Decreto 1377 de 2013: "Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas." (http://www.suin-juriscol.gov.co)

Ley 1273 de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien

jurídico tutelado - denominado ‘de la protección de la información y de los datos’- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones”. (http://www.suin-juriscol.gov.co)

Ley 527 de 1999: “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”. (http://www.suin-juriscol.gov.co)

Decreto 1747 de 2000: “Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.” (http://www.suin-juriscol.gov.co)

2.5. Marco Demográfico

JAVESALUD IPS es una entidad de salud que cuenta con aproximadamente 300 usuarios que interactúan diariamente con los diferentes sistemas de información y herramientas ofimáticas de la entidad, el personal esta delegado en aproximadamente un 75% en la parte asistencial, y el otro 25% la parte administrativa.

2.6. Marco Geográfico

JAVESALUD IPS, es una entidad ubicada en la ciudad de Bogotá (Colombia), en la actualidad cuenta con 9 sedes de las cuales 8 son asistenciales y una la sede administrativa.

La sede administrativa se encuentra ubicada en el barrio Pasadena, las demás sedes llevan como nombre el respectivo barrio de ubicación, entre las que se encuentran la sede Santa Barbara, la sede Santa Beatriz, la sede Palermo Sur y la sede Ciudad Bolívar. En la Universidad Javeriana contamos con dos sedes, una externa y dos internas, la externa con servicios de primer nivel, y las internas correspondientes a el centro de formación deportiva y el centro de atención psicológica, para finalizar dos sedes adscritas a seguros Allianz, una ubicada en el barrio salitre y la otra en el

barrio Navarra.

2.7. Estado del arte

2.7.1. Referentes Nacionales

A continuación, se referencian antecedentes y trabajos relacionados a nivel Nacional.

- John Jairo Perafán Ruiz, Mildred Caicedo Cuchimba desarrollaron el proyecto "Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca" para realizar el análisis de riesgos que permita generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en la Institución Universitaria Colegio Mayor del Cauca en la ciudad de Popayán.
- Jorge Luis Galeano villa, Cristian camilo Alzate Castañeda desarrollaron el proyecto "Protocolo de políticas de seguridad informática para las universidades de Risaralda" cuyo propósito fue construir y proponer un protocolo para la elaboración de una política seguridad informática para instituciones de educación superior en Risaralda.
- Juan David Aguirre Cardona, Catalina Aristizábal Betancourt presentaron el proyecto "Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda" su objetivo general fue diseñar el sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda en la ciudad de Pereira.

2.7.2. Referente internacional

Se referencian también antecedentes y trabajos relacionados a nivel Internacional.

- Hernández Pinto María Gabriela presentó su proyecto "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial su Objetivo general es diseñar un plan estratégico de seguridad de información para una empresa comercial. En la ciudad de

Guayaquil Ecuador.

- Magdalena Reyes Granados presenta su proyecto “Propuestas para impulsar la seguridad informática en materia de educación” su objetivo es realizar una investigación que permita estudiar, analizar y determinar la situación actual de la seguridad informática en México y su contraste a nivel internacional. En Ciudad de México en octubre del año 2011.

3. Metodología

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información esto permitirá realizar el estudio pertinente sobre los activos lógicos de JAVESALUD IPS.

3.1. Fases del trabajo de grado

En el desarrollo del proyecto se plantea la utilización de una metodología compuesta por tres fases principales,

3.1.1. Fase de planificación

En la fase de planeación se pretende recopilar y realizar el inventario de los activos lógicos de la entidad, esto se realizará a través de varios métodos entre los cuales se utilizará la entrevista individual y estructurada con las diferentes personas encargadas de la información, donde se buscará conocer la situación de los activos lógicos desde el punto de vista de estas personas, así mismo se realizará la verificación de los documentos que al respecto se encuentren en la entidad. En esta fase además se pretende realizar la programación de los procesos de seguridad sobre la información ya que es necesario no interferir con la adecuada funcionalidad de los procesos de la entidad.

3.1.2. Fase de Análisis de riesgos.

En la fase de ejecución se iniciará con el proceso de verificación y clasificación de riesgos, en este orden, se utilizarán las herramientas necesarias para este proceso, implementando la metodología de análisis y gestión de riesgos de sistemas de información Magerit.

3.1.3. Fase de Gestión de riesgos.

Se procede a elaborar un informe con los controles generados a partir de las matrices de riesgos y la evaluación generada a través de la metodología, estos controles se documentarán y se entregaran como informe final, y será la alta gerencia en base a su capacidad y gobernabilidad quien determinara la implementación o no de los controles.

3.1.4. Instrumentos o herramientas utilizadas

Como técnicas e instrumentos para llevar a cabo el desarrollo de los objetivos se tendrán en cuenta para la recopilación de la información y ejecución de las actividades a desarrollar, tales como: Entrevistas, Encuesta y Análisis de documentos.

Entrevista

Se realizará la entrevista con el gerente de tecnología, una entrevista individual y estructurada, que pretende identificar las características actuales posee el sistema de información desde el punto de vista de la gerencia de tecnología.

Análisis de documentos:

El análisis de documentos se realizara a través de un método cualitativo ya que en un análisis previo y superficial se determinó que no existen actualmente documentación exclusiva acerca de la seguridad informática de los activos lógicos de la entidad, por lo tanto se estudiarán los documentos necesarios que tenga la Entidad para determinar y conocer software, bases de datos, repositorios de archivos, carpetas compartidas y demás información que sea necesaria y que se encuentren alojados en dichos servidores, además de ejecuciones de backup y planes de recuperación de información en posibles desastres de perdida, esta información se extraerá mediante el plan de gestión documental ya instaurado por la entidad.

Herramientas de seguridad informática:

Las herramientas de seguridad informática que se utilizaran serán las que comprenda el método

expuestos en la fase de ejecución, en nuestro caso la metodología MAGERIT 3.0 y su catálogo de elementos y guía de técnicas.

PILAR

PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.

4. Desarrollo de la propuesta

Magerit utiliza tres procesos fundamentales, Planificación (P1), Análisis de riesgo (P2) y gestión del riesgo (P3), Con P1 iniciamos el proyecto sin embargo P3 es una tarea que se desarrolla permanentemente de acuerdo con los resultados del proceso P2, es decir que este proceso está alimentando la tarea de P3 constantemente, esto genera la gestión del riesgo supone la alteración del conjunto de controles, creando nuevos o modificando los existentes.

4.1. Actividades preliminares o Planeación (P1)

4.1.1. Estudio de oportunidad

La realización de un estudio de riesgos de los activos lógicos es necesario en la entidad JAVESALUD ya que no se cuenta actualmente con ningún proyecto o proceso relacionado con ese tema, esto generara adicionalmente la motivación a la alta dirección para implementar un SGSI completo.

4.1.2. Determinación del alcance del proyecto

Los objetivos descritos en la evaluación de los riesgos mediante la metodología están direccionados de acuerdo a lo establecido en el numeral 1.7 del presente documento, donde se pretende realizar mediante la metodología magerit el análisis de riesgos y vulnerabilidades de los activos lógicos de la entidad.

El Dominio del proceso se enfoca en los activos lógicos de la entidad y está limitado a estos activos, como resultado final se podrá determinar los controles que pueden mitigar los riesgos y las vulnerabilidades encontradas en el proceso.

Validando su entorno JAVESALUD IPS cuenta con una serie de procesos los cuales podríamos determinar cómo activos esenciales, cada uno de ellos administra ciertos activos lógicos, los cuales serán objeto de nuestro estudio.

Tabla 1 Macroproceso DG

Macroproceso	**Direccionamiento y Gerencia**
Procesos	DG-GEO - Gestión Externa de la Organización DG-GF - Gestión Financiera DG-GIO - Gestión Interna de la organización DG-RSE - Responsabilidad Social

Tabla 2 Macroproceso AT

Macroproceso	**Asistencial**
Procesos	AT-CT - Control Técnico AT-GC - Gestión Clínica AT-RC - Referencia y Contrarreferencia de la Red

Tabla 3 Macroproceso AC

Macroproceso	**Académico**
Procesos	AC-GCD - Gestión de los convenios Docencia-Servicio AC-GP - Gestión de prácticas formativas AC-IC - Investigación

Tabla 4 Macroproceso GH

Macroproceso	**Gestión Humana**

Procesos	GH-BI - Bienestar GH-CR - Compensación y relaciones laborales GH-FE - Formación y entrenamiento GH-SD - Selección y Desarrollo GH-SS - Salud y Seguridad en el trabajo

Tabla 5 Macroproceso AD

Macroproceso	**Administrativo**
Procesos	AD-CO - Compras, Activos Fijos e Inventarios AD-GA - Gestión Administrativa AD-GAF - Gestión del Ambiente físico AD-GET - Gestión de equipos y tecnología biomédica AD-GT - Gestión de Tecnología, información y Comunicaciones

Tabla 6 Macroproceso OC

Macroproceso	**Operaciones y Calidad**
Procesos	OC-ARE - Acceso, Registro, Espera y Egreso OC-GO - Gestión de Operaciones OC-GSP - Gestión de la Segur.del Paciente y Control del riesgo

	OC-INF - Información al paciente y su familia OC-PRO - Gestión de Proveedores de la Red Externa OC-SC - Servicio al Cliente OC-SGI - Sistema de Gestión Integral OC-SM - Seguimiento y Mejora continua de la Calidad OC-SUH - Mantenimiento del Sistema único de Habilitación

Marco Presupuestal

Tabla 7 Presupuesto global de la propuesta por fuentes de financiación (en miles de $).

RUBROS	VALOR UNITARIO	VALOR TOTAL
PERSONAL	$ 30.000	$ 28’800.000
EQUIPOS	$ 1’500.000	$ 2’400.000
SOFTWARE	N/A	N/A
MATERIALES	$ 200.000	$ 200.000
SALIDAS DE CAMPO	N/A	N/A
MATERIAL BIBLIOGRÁFICO	N/A	N/A
PUBLICACIONES Y PATENTES	N/A	N/A
SERVICIOS TÉCNICOS	N/A	N/A
VIAJES	N/A	N/A
CONSTRUCCIONES	N/A	N/A

MANTENIMIENTO	N/A	N/A
ADMINISTRACION	N/A	N/A
TOTAL	$ 1’730.000	$ 31’400.000

Tabla 8 Descripción de los gastos de personal (en miles de $).

INVESTIGADOR / EXPERTO / AUXILIAR	FORMACIÓN ACADÉMICA	FUNCIÓN DENTRO DEL PROYECTO	DEDICACIÓN Horas/semana	VALOR
INVESTIGADOR	INGENIERO DE SISTEMAS	EJECUTOR	20 HORAS SEMANALES	$ 30.000
INVESTIGADOR	INGENIERO DE SISTEMAS	EJECUTOR	20 HORAS SEMANALES	$ 30.000
TOTAL	$ 900.000			

Tabla 9 Descripción de los equipos que se planea adquirir (en miles de $).

EQUIPO	JUSTIFICACIÓN	VALOR TOTAL
N/A	N/A	N/A
TOTAL		

Tabla 10 Descripción y cuantificación de los equipos de uso propio (en miles de $)

EQUIPO	VALOR TOTAL
EQUIPO PORTÁTIL X 2	$ 1’800.000
IMPRESORA	$ 600.000

TOTAL	$ 2’400.000

Tabla 11 Descripción del software que se planea adquirir (en miles de $).

SOFTWARE	JUSTIFICACIÓN	VALOR TOTAL
N/A	N/A	N/A
TOTAL		

Tabla 12 Descripción y justificación de los viajes (en miles de $).

LUGAR / NO. DE VIAJES	JUSTIFICACIÓN	PASAJES ($)	ESTADÍA ($)	TOTAL, DÍAS	TOTAL
N/A	N/A	N/A	N/A	N/A	N/A
TOTAL					

Tabla 13 Valoración de las salidas de campo (en miles de $).

ITEM	COSTO UNITARIO	#	TOTAL
N/A	N/A	N/A	N/A
TOTAL			

Tabla 14 Materiales y suministros (en miles de $)

MATERIALES	JUSTIFICACIÓN	VALOR TOTAL
RESMA PAPEL	IMPRESIÓN DE DOCUMENTOS	$ 10.000
INSUMOS IMPRESORA	IMPRESIÓN DE DOCUMENTOS	$ 40.000

TOTAL	$ 50.000

Tabla 15 Bibliografía (en miles de $).

ÍTEM	JUSTIFICACIÓN	VALOR TOTAL
N/A	N/A	N/A
TOTAL		

Tabla 16 Servicios Técnicos (en miles de $).

TIPO DE SERVICIOS	JUSTIFICACIÓN	VALOR TOTAL
N/A	N/A	N/A
TOTAL		

4.1.3. Planificación del proyecto

El proyecto basara su planificación mediante la elaboración de entrevistas a los diferentes líderes de los procesos con el fin de determinar información relevante que nos permita abordar los objetivos del proyecto de la manera más eficaz y eficiente posible.

Los principales involucrados en el proceso tendrán varios frentes, desde el frente empresarial se realizara la participación de la gerencia de tecnología e información encabezada por el Ing. Carlos Nontoa, la gerencia de Operaciones y Calidad encabezada por la Dra. Mónica Leal, Dirección Médica encabezada por la Dra. Aida Gutiérrez, Gestión del riesgo encabezada por Viviana Cabrejo, Gestión de información área encargada al Ing. Javier Joya y las demás personas de soporte y análisis que se desprende de estas dependencias.

Desde el frente universitario se evidencia la participación de la Ing. Alexandra López quien se

encargará de la asesoría y supervisión de proyecto, finalizando con el frente estudiantil representado por los Ing. Javier Joya y Carlos Sacristán quienes serán los principales desarrolladores y realizarán la sustentación del proceso realizado.

Planificar el trabajo

4.1.4. Lanzamiento del proyecto

Las encuestas se realizaron a los diferentes líderes de procesos, con el fin de determinar que tanto se encuentra el personal involucrado en la seguridad informática de sus herramientas de trabajo. Por tal motivo se estructuro el sistema de encuestas en tres niveles diferentes

a). En primera instancia se determinó el nivel de alta gerencia, validando la capacidad que desde este ámbito se tiene frente al tema de seguridad de la información, la participación en la encuesta se determinó basados en el número de integrantes del comité directivo de la entidad, se determino tomar la muestra del 100% teniendo en cuenta que el numero de participantes es de 6 miembros, y generar una muestra menor no permitiría un mayor nivel de asertividad.

Ilustración 4 Encuesta Alta Gerencia

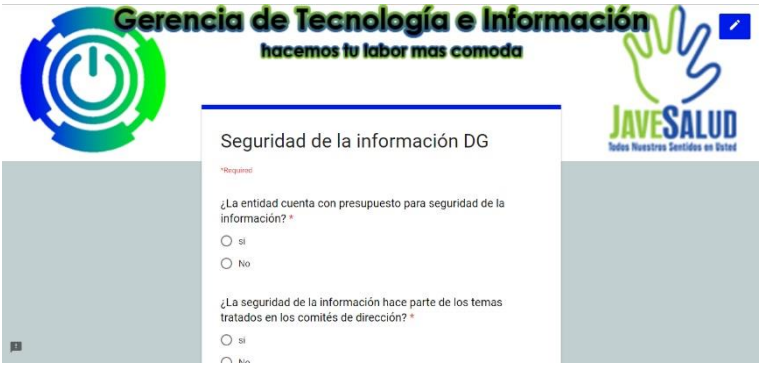
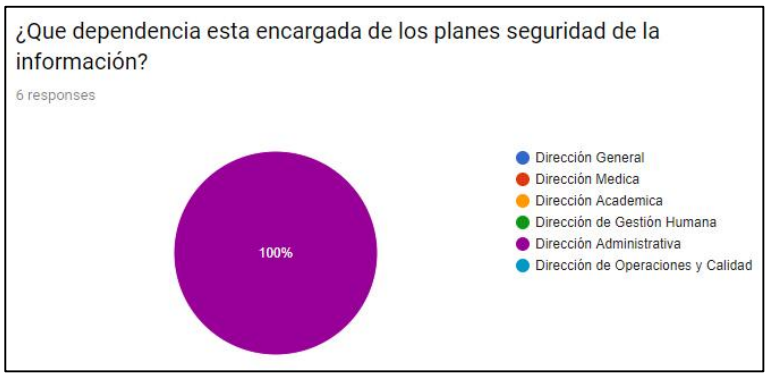
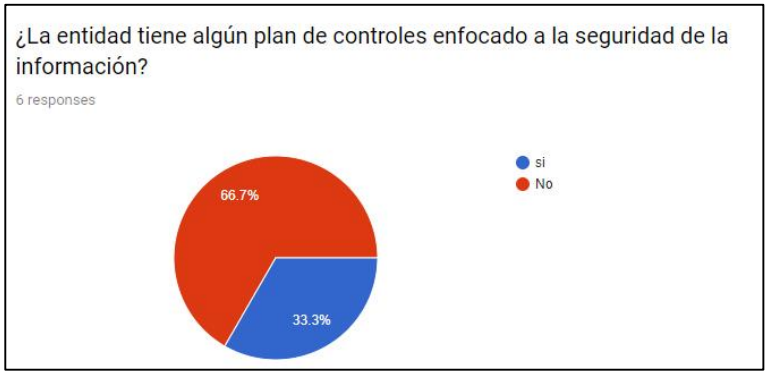


Ilustración 5 Pregunta 1 Encuesta Alta Gerencia



Para el comité directivo es claro quien o quienes deberían administrar la información y planes referentes a la seguridad de la información, lo que permite deducir que el direccionamiento de la información y novedades respecto al tema esta clarificado.

Ilustración 6 Pregunta 2 Encuesta Alta Gerencia



Se determina a la vez, que el comité directivo conoce el plan de controles de la entidad, pero a criterio individual determinan si afecta o no al tema de seguridad informática, donde la mayoría determino que el plan de controles de la entidad no tiene en cuenta una política de seguridad informática.

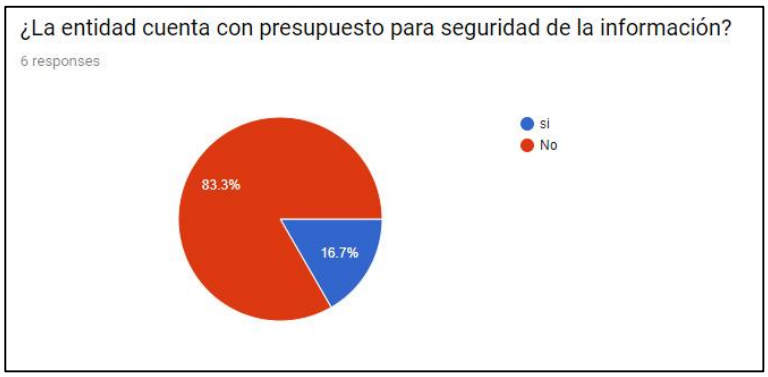
Ilustración 7 Pregunta 3 Encuesta Alta Gerencia

Así mismo la mayoría tiene entendimiento de los riesgos de los objetivos estratégico de la entidad basados en la seguridad informática, pero a su vez una minoría determino que para conocer los riesgos se debería tener un análisis estructurado y teniendo en cuenta que no existe, no se podría determinar los verdaderos riesgos.

Ilustración 8 Pregunta 4 Encuesta Alta Gerencia

Debido a la naturaleza de la entidad, las reuniones de los comités directivos se enfocan en su mayoría a tratar y administrar temas asistenciales, lo que genera que el tema de seguridad informática no sea de prioridad para la entidad, la validación de las respuestas da a entender que no se tiene claro hasta que punto lo tratado hace referencia a seguridad de la información.

Ilustración 9 Pregunta 5 Encuesta Alta Gerencia



En cuanto a presupuesto se determinó a futuro realizar las inversiones ya que la entidad acaba de pasar por un proceso de habilitación donde tuvo que realizar inversiones de urgencia, y debió suspender algunos proyectos, aunque una gran minoría del comité determino que la inversión e seguridad no es de gran impacto en las finanzas de la entidad.

b). En segundo nivel, y como siguiente orden jerárquico se encuentra la instancia de líderes de procesos y gerentes, que determinara el estado actual y preparación frente a riesgos.

Javesalud en su esquema organizacional se compone de 29 procesos definidos liderados y gerenciados por 12 colaboradores de la entidad, lo que permite al igual que en la encuesta de alta gerencia realizar una toma de muestra del 100% .

Ilustración 10 Encuesta Nivel Gerencial

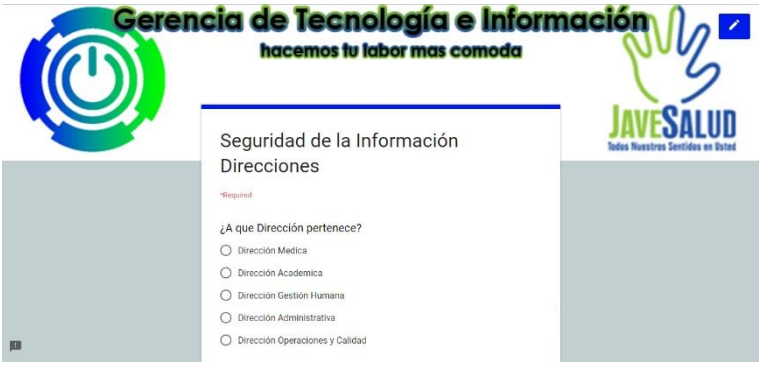
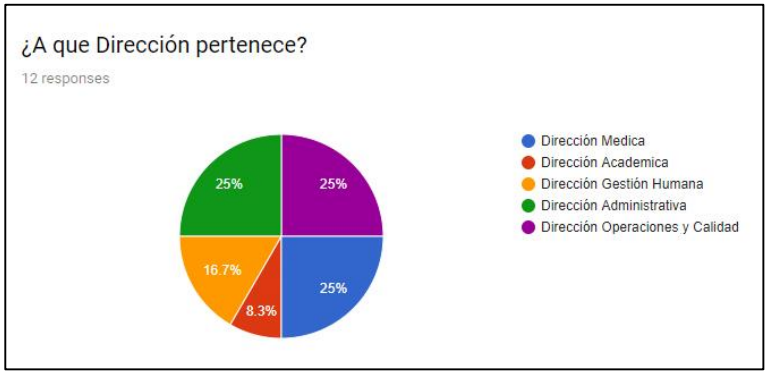
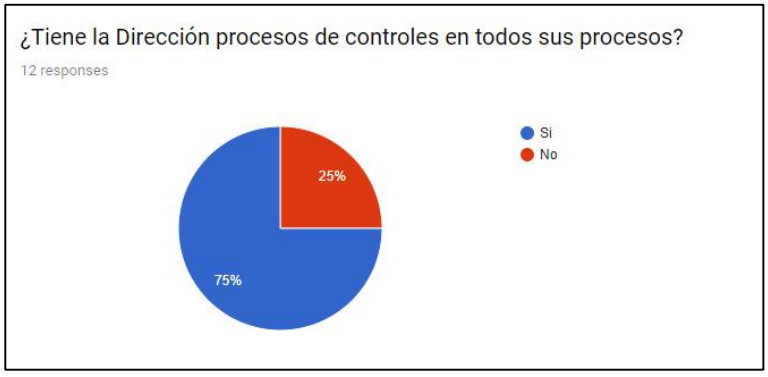


Ilustración 11 Pregunta 1 Encuesta Nivel Gerencial



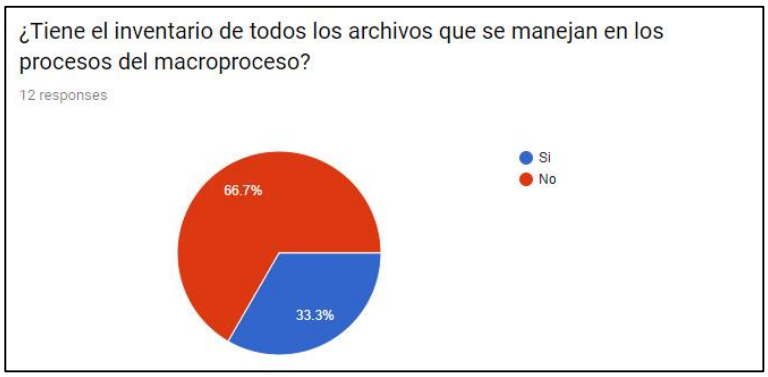
La primera pregunta nos muestra claramente las tres direcciones que mas procesos maneja, mostrando claramente el core del negocio en la dirección médica, y aunque a pesar de ser parte de la misión de la entidad la dirección académica es la que menos procesos ejecuta.

Ilustración 12 Pregunta 2 Encuesta Nivel Gerencial



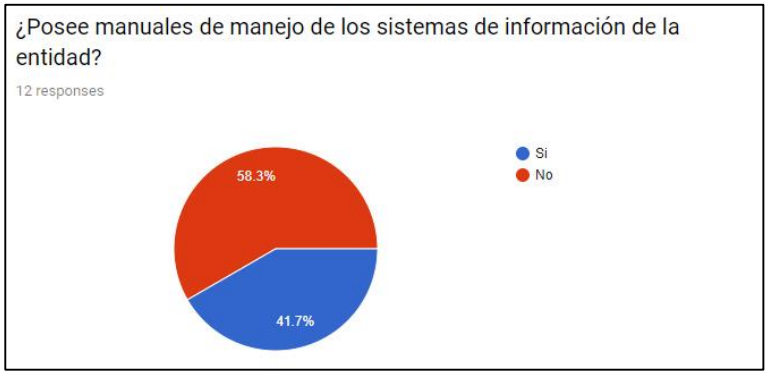
Los diferentes lideres y gerentes en su mayoría concuerdan en considerar que tienen todos sus procesos controlados, sin embargo, un pequeño numero considera que hay que reforzar los controles de sus procesos.

Ilustración 13 Pregunta 3 Encuesta Nivel Gerencial



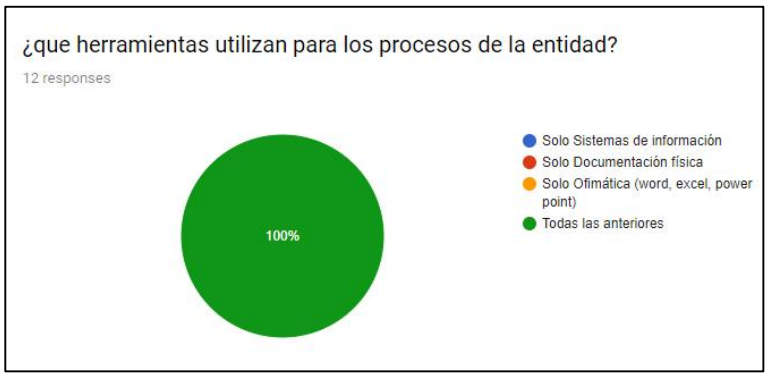
Así mismo y como complemento de la justificación del proyecto, los líderes y gerentes de los procesos a pesar de tener un sistema de documentación, no tienen una identificación plena de los activos de información que manejan

Ilustración 14 Pregunta 4 Encuesta Nivel Gerencial



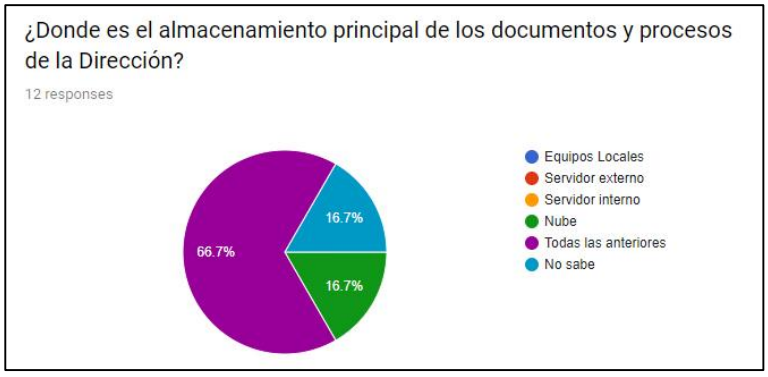
Teniendo en cuenta que la mayoría de sistemas de información que se manejan en la entidad son de propiedad de terceros, los manuales tienen una contextualización básica del sistema, y son muy pocos los que han sido transcritos a un enfoque mas personalizado de los procesos,

Ilustración 15 Pregunta 5 Encuesta Nivel Gerencial



Se tiene claridad de manera unánime en cuanto a que todos los procesos manejan diversidad de tipos de activos, lo que genera que el control sobre ellos deba ser más estructurado y planeado,

Ilustración 16 Pregunta 6 Encuesta Nivel Gerencial



Para finalizar la encuesta de nivel gerencial, se realiza una pregunta que pretende identificar la capacidad y calidad de almacenamiento de activos en cada uno de los procesos, aunque en su mayoría los lideres y gerentes de procesos reconocen los diferentes niveles de almacenamiento que maneja la entidad, también existe un grupo minoritario que no posee la información pertinente o completa sobre el tema.

c). Y para finalizar la instancia de ultimo nivel que abarca los niveles operativos y pretende validar la preparación de los trabajadores en cuanto a administración de seguridad en sus labores diarias, en vista de que esta encuesta es más amplia, es necesario realizar el estudio realizando un

método de muestreo que nos permita optimizar el trabajo.

Javesalud tiene en su totalidad 325 colaboradores distribuidos en 275 de planta y 50 por prestación de servicios, lo cual nos direcciona a realizar un método de encuesta denominado, "método de muestreo probabilístico" que nos permita tomar una muestra significativa que cumpla con los requerimientos mínimos para desarrollar un análisis más cercano a la realidad.

Muestreo aleatorio simple

El muestreo aleatorio simple consiste en sacar un subconjunto del total de colaboradores de Javesalud, para realizar la distribución de la encuesta, esto con el fin de minimizar el trabajo y los análisis de poblaciones de mayor cantidad.

Para el numero de la muestra adecuados utilizamos la fórmula para cálculo de muestra de poblaciones finitas, teniendo en cuenta que según información obtenida por la dirección de gestión humana la población conocida de la entidad es de 325 colaboradores, sobre la cual se ejecutara la siguiente formula de muestreo aleatorio simple.

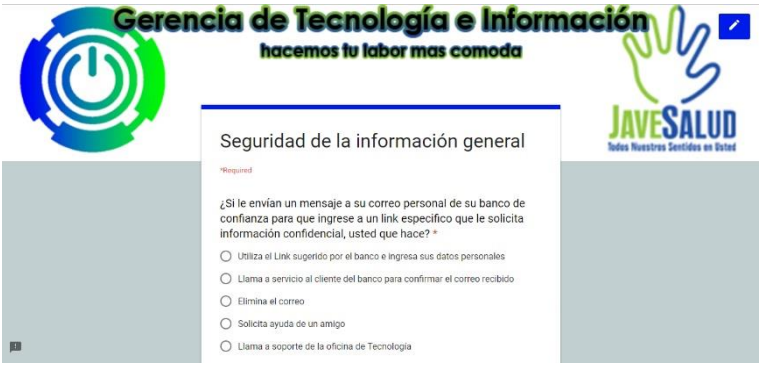
Ilustración 17 Formula para cálculo de la muestra poblaciones finitas

$$n = \frac{N \times Z_a^{\,2} \times p \times q}{d^2 \times (N-1) + Z_a^{\,2} \times p \times q}$$

N representa el numero de la población total, Z es el nivel de confianza que radica en la posibilidad de que rangos aleatorios de muestras contengan la media de estas muestras, p es la probabilidad de éxito, que la probabilidad de fracaso y d es el margen de error.

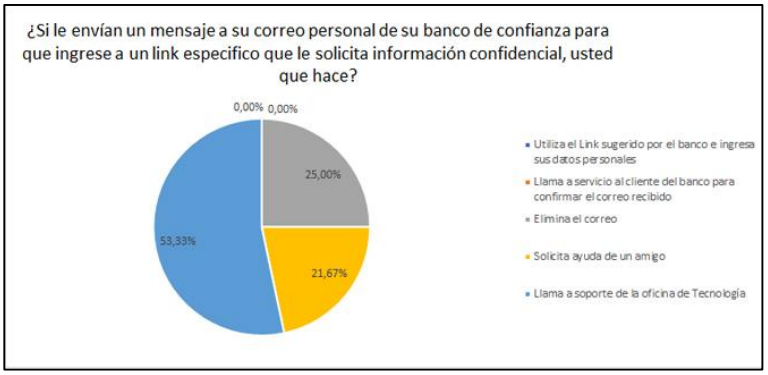
Al generar los cálculos de la formula, podremos determinar que la muestra que nos permitirá realizar un análisis más eficaz se generará a partir de 60 registros aleatorios, si tomamos los valores de nivel de confianza y probabilidades en un nivel estándar de 50% de probabilidades.

Ilustración 18 Encuesta Nivel Operacional



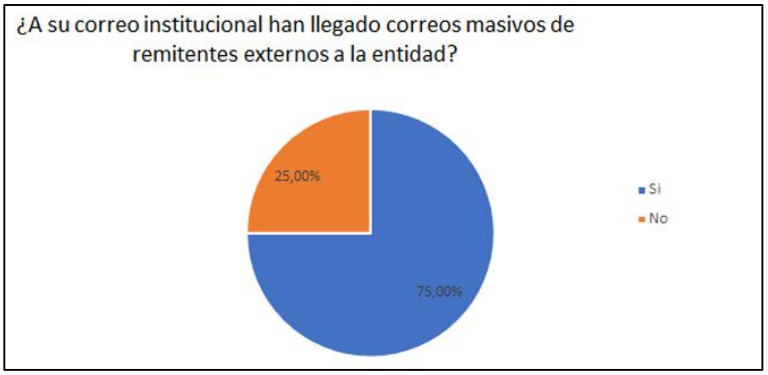
Fuente: GARAVITO (octubre 2015)

Ilustración 19 Pregunta 1 Encuesta Nivel Operativo



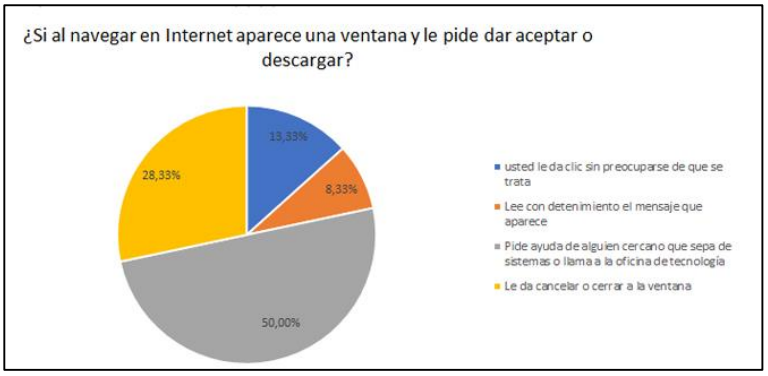
Uno de los procesos que se tiene mas claro es la búsqueda de ayuda en las personas encargadas de las novedades, por lo cual los mensajes de correo que presentan algún tipo de estado extraño es reportado por la mayoría de colaboradores de la entidad.

Ilustración 20 Pregunta 2 Encuesta Nivel Operativo



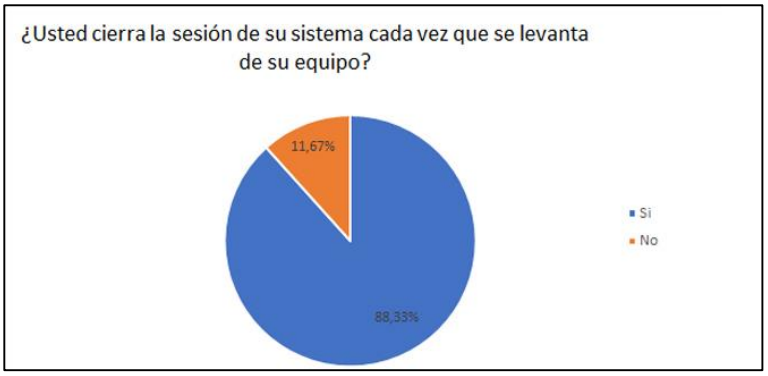
Javesalud IPS es una entidad encargada de los servicios de salud, por lo cual posee una gran cantidad de información sensible, en el caso de la atención en salud de sus pacientes, que la hace atractiva a los cazadores de bases de datos, por lo cual recibe bastantes correos con procedencia sospechosa.

Ilustración 21 Pregunta 3 Encuesta Nivel Operativo



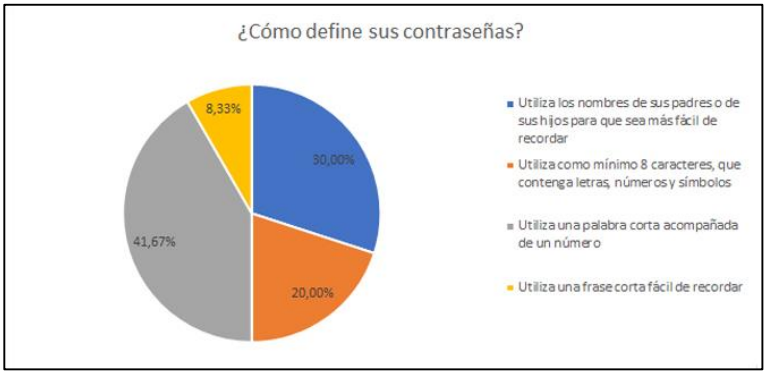
Se reafirma la capacidad de los colaboradores de tener claridad en que este tipo de situaciones debe ser informada a los especialistas en tecnología, que se evidencia en el porcentaje de participación, pero es necesario reforzar estos conceptos en todas las áreas.

Ilustración 22 Pregunta 4 Encuesta Nivel Operativo



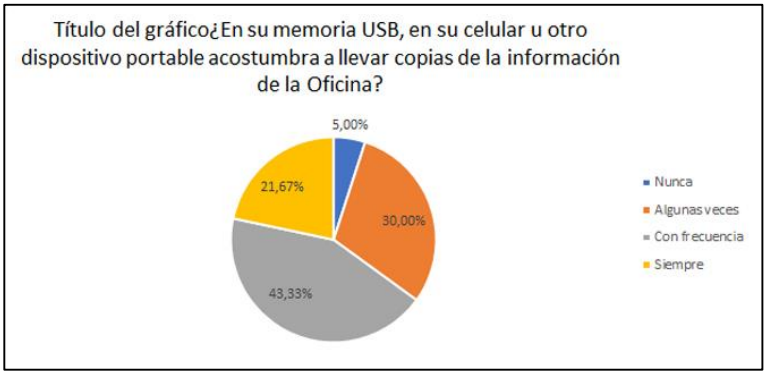
Los colaboradores de Javesalud, son conscientes de la necesidad de protección de datos no solo a nivel externo sino interno, y eso genera algunas costumbres que a pesar de no estar documentadas son de conocimiento de ellos.

Ilustración 23 Pregunta 5 Encuesta Nivel Operativo



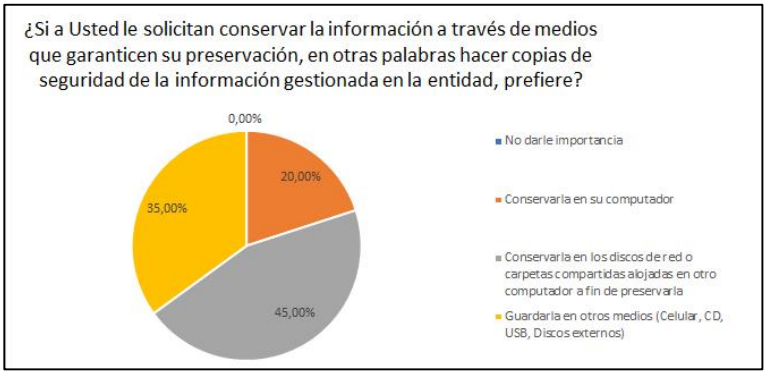
El dominio de Javesalud, exige a los colaboradores que utilizan la tecnología una serie de características en la contraseña para ser validada, estas reglas son interpretadas y utilizadas por los colaboradores según su diferente forma de generar una contraseña.

Ilustración 24 Pregunta 6 Encuesta Nivel Operativo



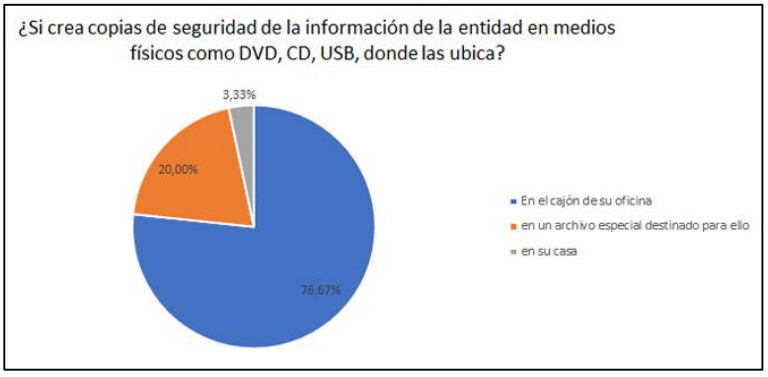
Es usual que los colaboradores utilicen sus dispositivos para tener un backup personal de su información, sin embargo esta información son archivos locales que no pertenecen a los sistemas de información.

Ilustración 25 Pregunta 7 Encuesta Nivel Operativo



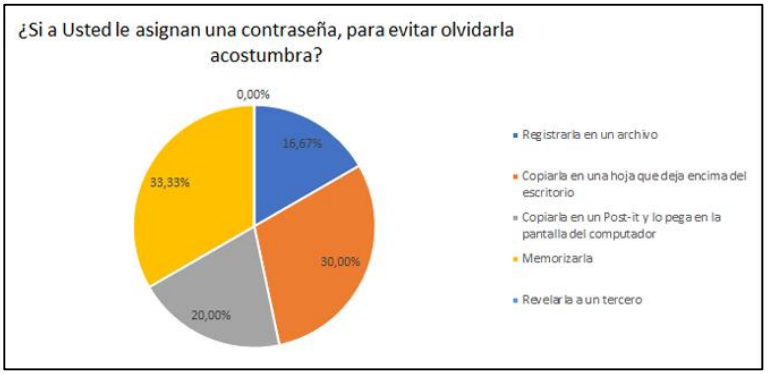
A pesar de que los colaboradores están acostumbrados a guardar cierta parte de su información laboral en sus dispositivos personales, la principal fuente de almacenamiento de backups son los propios servidores establecidos para eso.

Ilustración 26 Pregunta 8 Encuesta Nivel Operativo



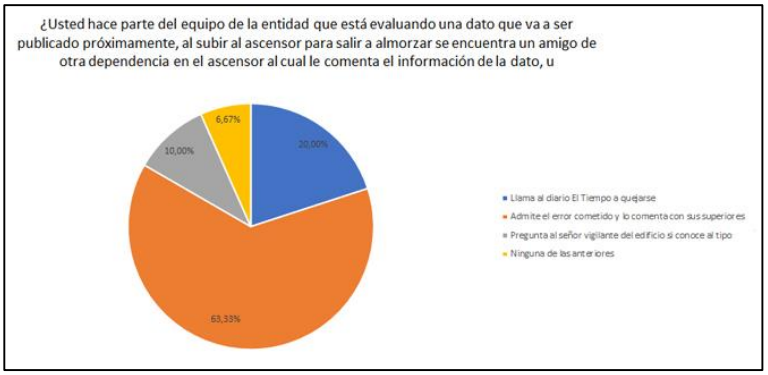
Es también una tendencia en los colaboradores guardar sus backups en la entidad, evitando el compromiso de realizar traslados de información a sus hogares

Ilustración 27 Pregunta 9 Encuesta Nivel Operativo



Una de las costumbres que se evidencian que puede salir del concepto de seguridad es la necesidad de plasmar las contraseñas para recordarlas.

Ilustración 28 Pregunta 10 Encuesta Nivel Operativo

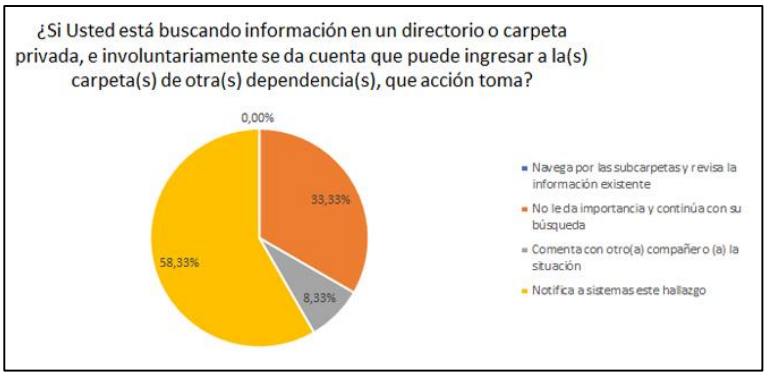


Otro proceso que se tiene claro en la entidad es el conducto regular para las novedades presentadas respecto a los procesos de la información.

Ilustración 29 Pregunta 11 Encuesta Nivel Operativo

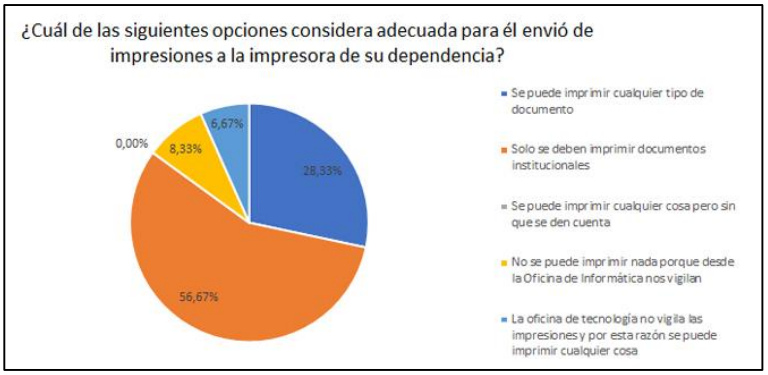
Es importante reconocer los responsables de la información de los empleados de la empresa, y la entidad tiene claro quienes manejan este tipo de datos.

Ilustración 30 Pregunta 12 Encuesta Nivel Operativo



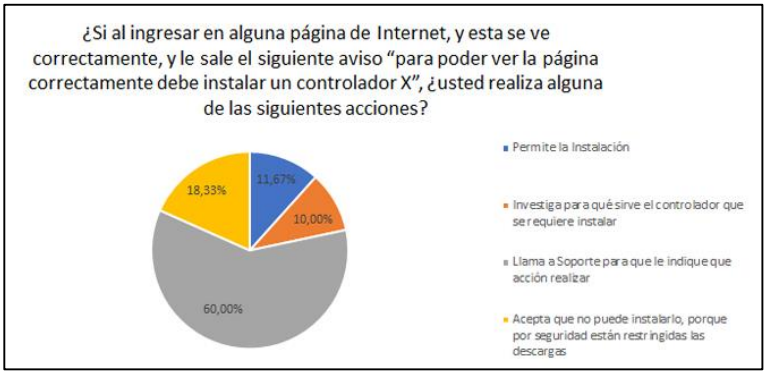
Los colaboradores no solo conocen el direccionamiento de las novedades de la información, sino que la mayoría son consientes del riesgo que se corre si no se informa de este tipo de novedades.

Ilustración 31 Pregunta 13 Encuesta Nivel Operativo



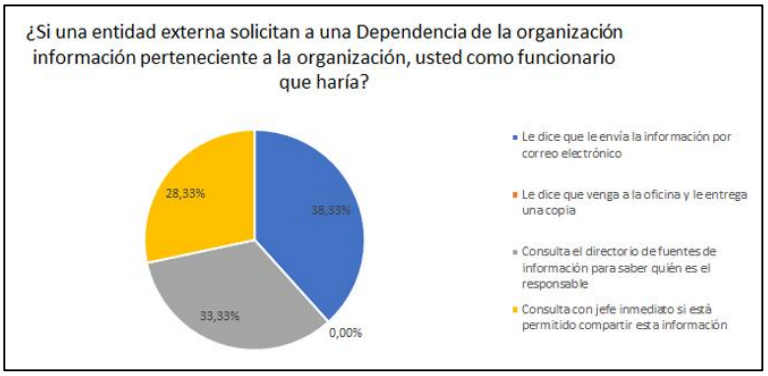
La utilización de los elementos de la entidad es de uso principal de la propia entidad y los colaboradores en su mayoría reconocen esta directiva.

Ilustración 32 Pregunta 14 Encuesta Nivel Operativo



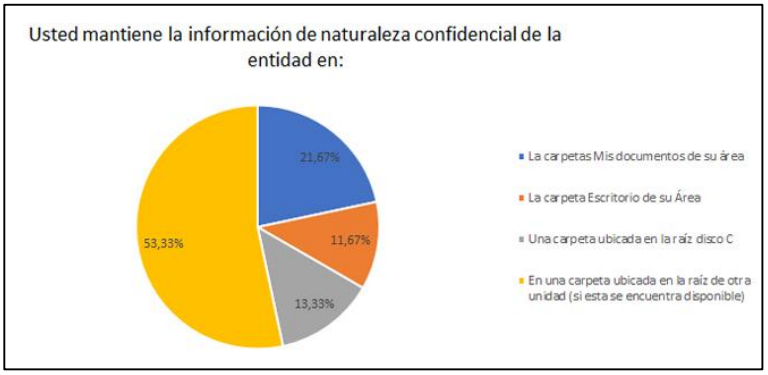
A pesar de que las políticas de instalación de software y controladores plasman la necesidad de ser instaladas desde un usuario administrador, los colaboradores son conscientes de la obligación de informar a las personas idóneas para realizar este tipo de procesos.

Ilustración 33 Pregunta 15 Encuesta Nivel Operativo



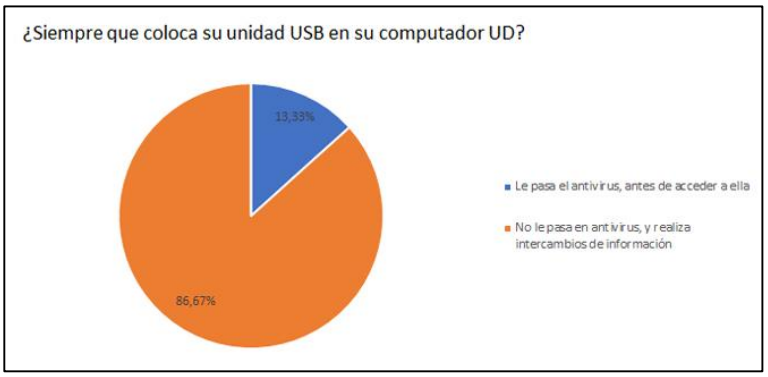
Uno de los procesos que aun no se tiene claro es la forma de solicitar la información por parte de los agentes externos, ya que se tiene un proceso establecido de solicitud y a la vez un responsable de entregar esa información.

Ilustración 34 Pregunta 16 Encuesta Nivel Operativo



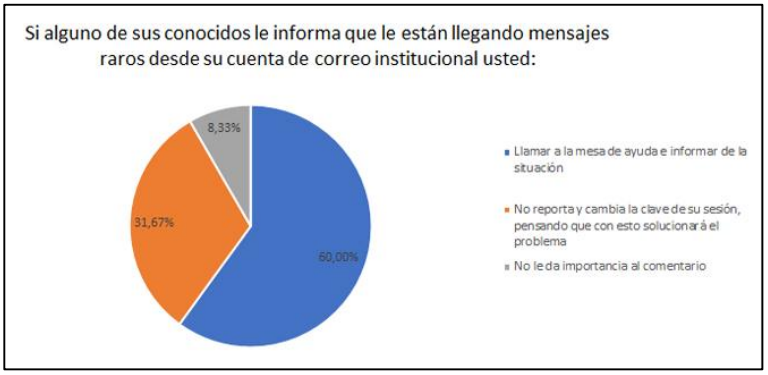
Las carpetas compartidas de servidores de almacenamiento son las mas utilizadas a la hora del almacenamiento, ya que se posee una política no documentada de los permisos y roles de acceso a estas carpetas, lo que genera en los colaboradores la confianza sobre estas carpetas.

Ilustración 35 Pregunta 17 Encuesta Nivel Operativo



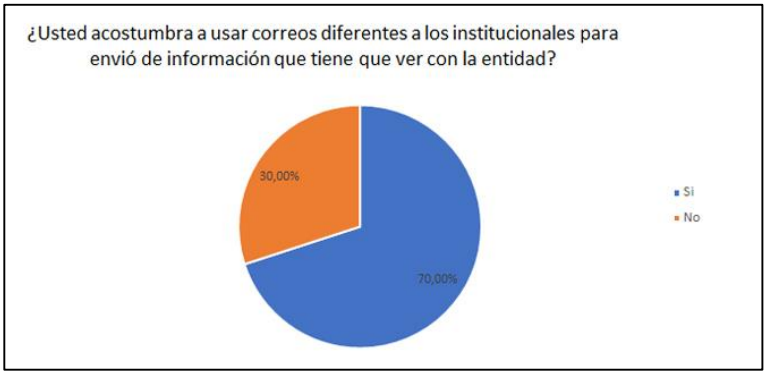
Uno de los procesos menos utilizados es el que tiene que ver directamente con los usuarios, como la necesidad de analizar los dispositivos extraíbles esta costumbre aun no se ha adoptado por los colaboradores de la entidad.

Ilustración 36 Pregunta 18 Encuesta Nivel Operativo



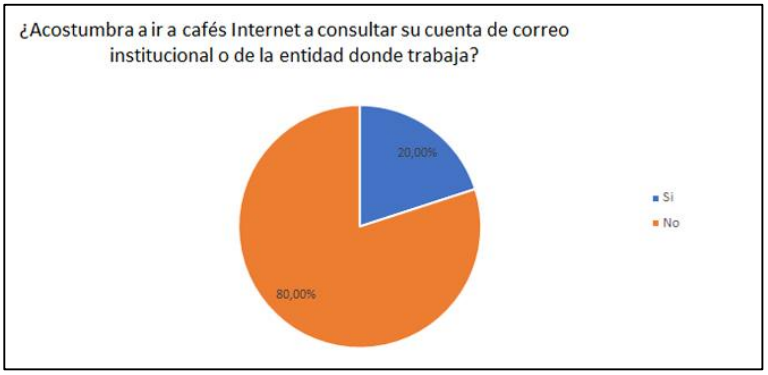
A pesar de no tener la esencia de seguridad ya que los colaboradores determinan mas esta novedad como soporte técnico mas que como falla de internet, si es claro que el proceso y conducto siguen siendo claros para los colaboradores

Ilustración 37 Pregunta 19 Encuesta Nivel Operativo



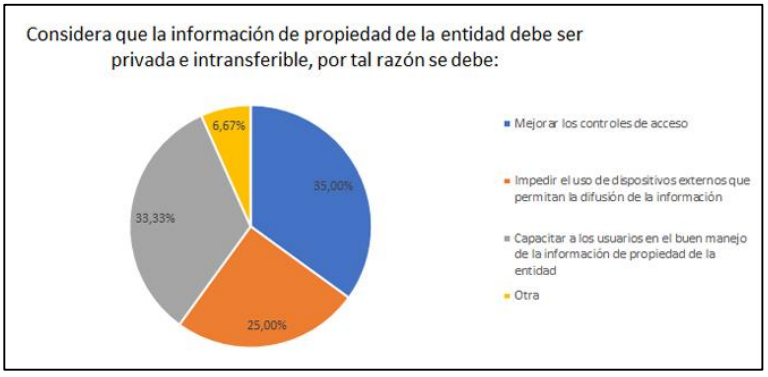
Javesalud maneja información de alto nivel de tamaño y en alguna ocasión esta información no tiene los medios de trasmisión a través del servidor propio de correo por lo que es necesario utilizar servidores de correo comerciales.

Ilustración 38 Pregunta 20 Encuesta Nivel Operativo



Una de las políticas personales que manejan los colaboradores de la entidad es manejar la información empresarial de uso exclusivo de la entidad y no realizar actividades laborales en su entorno personal.

Ilustración 39 Pregunta 21 Encuesta Nivel Operativo



En el análisis de la ultima pregunta se evidencia la misma constante de toda la encuesta y es que a pesar de que la mayoría conoce los procesos básicos de seguridad si es requerido un afianzamiento de conceptos en aquellas minoras que aun no realizan procesos adecuados de manejo de la información, además de la correcta documentación de estas políticas y su socialización.

Basados en esta información y con el fin de darle cumplimiento al alcance del proyecto, determinados en la tabla de activos de Magerit, la selección y filtro de los activos objetos de estudio

Tabla 17 Tipos de Activos según Magerit III

Tipo de Activo	**Descripción**
[Essential] Activos esenciales	Activos esenciales para la organización, información personal de individuos, y de normatividad y acceso.
[arch] Arquitectura del sistema	Establece la diferencia, requisitos y límites entre proveedor y usuario o entre usuario interno y externo
[D] Datos / Información	Datos almacenados en soportes de información.
[keys] Claves criptográficas	Proteger y autenticar el ingreso a través de claves.
[S] Servicios	Son las funciones que involucran las necesidades de un usuario
[SW] Aplicaciones (software)	Programas, aplicativos, desarrollos
[HW] Equipos informáticos (hardware)	Su concepto se basa principalmente en dispositivos de almacenamiento y procesamiento de activos.
[COM] Redes de comunicaciones	Centrándose en que son medios de transporte que llevan datos de un sitio a otro.
[Media] Soportes de información	Medios de almacenamiento de larga vida.

[AUX] Equipamiento auxiliar	Dispositivos que soportan procesos principales, como fuentes de alimentación eléctrica, muebles, etc.
[L] Instalaciones	Infraestructura física
[P] Personal	Factor Humano
XML	Abarca la capacidad de evolución tecnológica de los activos

Basados en la tabla de activos de Magerit, y como cumplimiento de los objetivos del proyecto nos enfocaremos principalmente en los activos lógicos de la entidad, y los procesos en los que se ven involucrados.

Dimensiones de Valoración

Tabla 18 Tabla Dimensiones de Valoracion

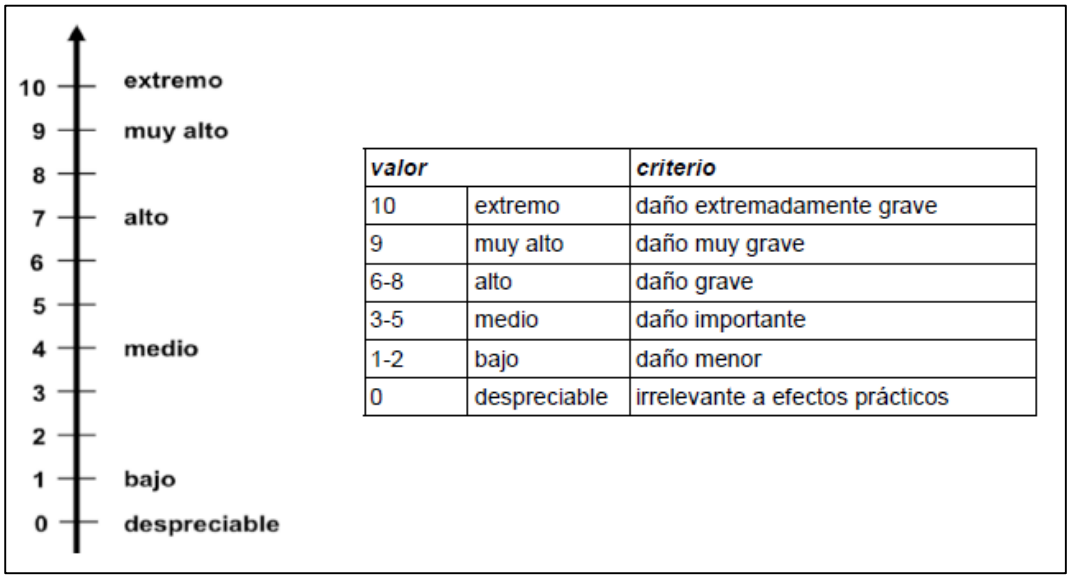
[D] disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

[T] trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Criterios de evaluación

Una de las formas de evaluación de activos que realiza la metodología Magerit es la evaluación de criterios subjetivos o a discreción del usuario, por lo que se sugiere una escala de 10 valores

Ilustración 40 Escala común de riesgos Magerit



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Así mismo se generan formas de evaluación más detalladas, que permiten evaluar de igual forma a los activos cuyo valor afecta mas de un área de la entidad.

Tabla 19 Niveles de Valoración - Información de Carácter Personal

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

Tabla 20 Niveles de Valoración - Obligaciones legales

[lpo]	**Obligaciones legales**	
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Tabla 21 Niveles de Valoración - Seguridad

[si]	**Seguridad**

10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Tabla 22 Niveles de Valoración - Intereses comerciales o económicos

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial

	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

Tabla 23 Niveles de Valoración - Interrupción del servicio

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Tabla 24 Niveles de Valoración - Orden Público

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

Tabla 25 Niveles de Valoración - Operaciones

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Tabla 26 Niveles de Valoración - Administración y gestión

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

Tabla 27 Niveles de Valoración - Perdida de Confianza

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones

	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Tabla 28 Niveles de Valoración - Persecución de delitos

[**crm] Persecución de delitos**		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

Tabla 29 Niveles de Valoración - Tiempo de recuperación del servicio

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

4.2. Análisis de riesgos (P2)

4.2.1. Inventario de activos de información

Los activos de software, encontrados en la parte lógica de la empresa son los siguientes:

En esta clasificación se encuentran los activos de información que se encuentran en la parte lógica de la empresa

Tabla 30 Identificación activos [SW]

Item	***[SW] Aplicaciones (software)***	***Descripción***
1	[browser_Js] navegador web	Navegador por defecto (Google Chrome)
2	[app_Js] servidor de aplicaciones	Se tienen instalados aplicativos como SAP, OFFICE, MAQUINAS VIRTUALES
3	[email_client_Js] cliente de correo electrónico	Contratación Officce 365
4	[oficce_Js] Ofimática.	Contratación de licenciamiento de herramientas ofimáticas
5	[av_Js] Antivirus	Software de protección contra virus, malware o codigos maliciosos.
6	[os_Js] sistema operativo	Licenciamiento de Sistemas Operativos encontrados en servidores y en equipo de empleados
7	[S_backup_Js] sistema de backup	Software de programación automática de backups

Tabla 31 Identificación activos [D]

Item	*[D] Datos / Información*	*Descripción*
1	[files] ficheros	Archivos relacionados con la continuidad ddl pc
2	[backup] copias de respaldo	Copias de respaldo de las bases de datos que actualmente se manejan en la IPS Javesalud
3	[password] credenciales (ej. contraseñas)	Credenciales de acceso para los respectivos usuarios de la empresa, ligados al directorio activo
4	[log] registro de actividad (2)	Logs del servidor de dominio y de la DB de SQL
5	[test] datos de prueba	Base de datos de pruebas para realizar compilaciones, que se encuentra alojada en un servidor propio.

Valoración de los activos:

Para poder determinar un nivel de criticidad de los activos y evaluar el impacto que estos puedan ocasionar, se hace necesario otorgar un nivel de valoración a cada activo lógico. El modelo Magerit sugiere trabajar cinco dimensiones o criterios de evaluación, que permita clasificar los activos, siendo los siguientes:

1. Confidencialidad
2. Integridad

3. Disponibilidad
4. Autenticidad
5. Trazabilidad

De las anteriores dimensiones, únicamente se utilizarán “confidencialidad, integridad y disponibilidad” siendo los pilares esenciales para brindar una criticidad a los activos lógicos de información.

La tabla de escalas sobre la cual se evaluará cada activo es la siguiente:

Tabla 32 Escala de valoración de los activos de la IPS Javesalud

Escala de valores		**Criterio del valor**
Muy alto	MA	Afecta en gran parte todo el proceso de operación involucrando daños graves
Alto	A	Afecta la operación de la organización en alto grado
Medio	M	Afecta el proceso de operación en un grado menor
Bajo	B	Afecta a la organización en un grado menor
Muy baja	MB	Sin afectación a la IPS Javesalud

(Fuente: Libro I Magerit v3)

De acuerdo al método a implementar para encontrar los activos más críticos, se realiza la asignación de la escala a los activos lógicos encontrados y se clasifica cada activo de acuerdo a su nivel de criticidad:

Tabla 33 Nivel de criticidad activos JAVESALUD

	Activos Logicos	***Descripcion***	***Confden.***	***Itegri.***	***Dispo.***
	[D] Datos / Información				
1	[files_Js] ficheros	Archivos relacionados con la continuidad de la empresa	A	A	M
2	[backup_Js] copias de respaldo	Copias de respaldo de las bases de datos que actualmente se manejan en la IPS Javesalud	MB	MA	M
3	[password_Js] credenciales (ej. contraseñas)	Credenciales de acceso para los respectivos usuarios de la empresa, ligados al directorio activo	A	A	M
4	[log_Js] registro de actividad (2)	Logs del servidor de dominio y de la DB de SQL	A	A	A
5	[test_Js] datos de prueba	Base de datos de pruebas para realizar compilaciones, que se	B	A	A

		encuentra alojada en un servidor propio.			
	[SW] Aplicaciones (software)				
6	[browser_Js] navegador web	Navegador por defecto (Google Chrome)	B	A	M
7	[app_Js] servidor de aplicaciones	Se tienen instalados aplicativos como SAP, OFFICE, MAQUINAS VIRTUALES	A	MA	MA
8	[email_client_Js] cliente de correo electrónico	Contratación Officce 365	A	A	M
9	[oficce_Js] Ofimática.	Contratación de licenciamiento de herramientas ofimáticas	A	M	M
10	[av_Js] Antivirus	Software de protección contra virus, malware o codigos maliciosos.	M	A	A
11	[os_Js] sistema operativo	Licenciamiento de Sistemas Operativos	M	A	A

		encontrados en servidores y en equipo de empleados			
12	[S_backup_Js] sistema de backup	Software de programación automática de backups	A	MA	M

4.2.2. Determinación de las amenazas y su eficacia

Identificación de las amenazas

Tabla 34 Identificación de amenazas [SW]

[ACTIVO]	[AMENAZA]
[browser_Js] navegador web	[I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas
[app_Js] servidor de aplicaciones	[I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software)

	[A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software)
[email_client_Js] cliente de correo electrónico	[E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software)
[oficce_Js] Ofimática.	[E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software)
[av_Js] Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas

	[I.5] Avería de origen físico o lógico.
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
[os_Js] sistema operativo	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.8] Difusión de software dañino
	[A.22] Manipulación de programas
	[I.5] Avería de origen físico o lógico.
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
[S_backup_Js] sistema de backup	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.8] Difusión de software dañino
	[A.22] Manipulación de programas
	[I.5] Avería de origen físico o lógico.
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
[browser_Js] navegador web	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.8] Difusión de software dañino
	[A.22] Manipulación de programas
	[I.5] Avería de origen físico o lógico.
[app_Js] servidor de aplicaciones	[E.8] Difusión de software dañino

	[E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico.
[email_client_Js] cliente de correo electrónico	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico.
[oficce_Js] Ofimática.	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico.
[av_Js] Antivirus	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software)

	[E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software)
[os_Js] sistema operativo	[E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas [I.5] Avería de origen físico o lógico. [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software)
[S_backup_Js] sistema de backup	[E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino [A.22] Manipulación de programas

Tabla 35 Identificación de amenazas [D]

[ACTIVO]	[AMENAZA]
[files] ficheros	[E.15] Alteración accidental de la información [E.18] Destrucción de información

[backup] copias de respaldo	[E.19] Fugas de información
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
[password] credenciales (ej. contraseñas)	[E.19] Fugas de información
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.19] Fugas de información
[log] registro de actividad (2)	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
[test] datos de prueba	[E.15] Alteración accidental de la información

	[E.18] Destrucción de información
	[E.19] Fugas de información
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

La tabla de degradación nos permite analizar que tato puede llegar a verse afectado el activo

Tabla 36 Degradación de los activos

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

La otra manera de evaluar las amenazas es la probabilidad de ocurrencia de estas.

Tabla 37 Probabilidad de ocurrencia amenazas

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años

MB	1/100	muy poco frecuente siglos

Tabla 38 Valoración de amenazas [SW]

[SW] Aplicaciones (software)	Amenazas	Prob	Degradación [D]	[I]	[C]	PROM.
[browser_Js] navegador web	[E.19] Fugas de Información	MB			A	A
	[E.20] Vulnerabilidades de los programas (software)	B	M	B	A	M
	[A.10] Antelación de secuencia	B		B		B
	[A.22] Manipulación de programas	B	M	MB	M	M
	[I.5] Avería de origen físico o lógico.	M	MA			MA
	[E.2] Errores del administrador	M	M	A	A	A
[app_Js] servidor de aplicaciones	[E.8] Difusión de software dañino	B	A	MA	A	MA
	[E.9] Errores de [re-]encaminamiento	B			MA	MA
	[E.20] Vulnerabilidades de los programas (software)	M	M	A	A	A
	[E.18] Destrucción de información	M	MA			MA

[email_client_Js] cliente de correo electrónico	[E.8] Difusión de software dañino	M	A	M	B	M
	[A.5] Suplantación de la identidad del usuario	B			MA	MA
	[E.1] Errores de los usuarios	M	B	M	MA	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	M	M	A		A
[oficce_Js] Ofimática.	[E.1] Errores de los usuarios	M	M	A	B	M
	[E.18] Destrucción de información	B	A			A
	[A.7] Uso no previsto	A	B	A	A	A
	[E.8] Difusión de software dañino	B	A	M	M	A
	[E.20] Vulnerabilidades de los programas (software)	M	A	M	M	A
[av_Js] Antivirus	[I.5] Avería de origen físico o lógico	M	A			A
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	A	B		M
[os_Js] sistema operativo	[E.20] Vulnerabilidades de los programas (software)	M	M	A	B	M
	[E.1] Errores de los usuarios	A	B	A	A	A
	[E.8] Difusión de software dañino	M	A	B	M	M

	[E.21] Errores de mantenimiento / actualización de programas (software)	M	A	M		A
	[A.8] Difusión de software dañino	B	A	A	A	A
	[A.11] Acceso no autorizado	B		MA	MA	MA
	[I.5] Avería de origen físico o lógico	B	A			A
[S_backup_Js] sistema de backup	[E.20] Vulnerabilidades de los programas (software)	B	A	A	B	A
	[E.19] Fugas de información	M			B	B
	[E.1] Errores de los usuarios	A	A	A	M	A

Tabla 39 Valoración de amenazas [D]

			Degradación			
[D] Datos / Información	Amenazas	Prob	[D]	[I]	[C]	PROM
	[E.1] Errores de los usuarios	M	A	A	B	A
[files] ficheros	[E.15] Alteración accidental de la información	A		MA		MA
	[A.6] Abuso de privilegios de acceso	M	B	A	M	M

	[A.18] Destrucción de información	B	MB			MB
[backup] copias de respaldo	[E.1] Errores de los usuarios	A	A	A	M	A
	[E.2] Errores del administrador	B	B	A	B	M
[password] credenciales (ej. contraseñas)	[A.5] Suplantación de la identidad del usuario	A			A	A
	[A.11] Acceso no autorizado	B		A	MA	MA
	[A.19] Revelación de información	M			MA	MA
[log] registro de actividad (2)	[A.15] Modificación deliberada de la información	B		A		A
	[A.6] Abuso de privilegios de acceso	B	B	A	A	A
	[A.11] Acceso no autorizado	B		A	A	A
	[E.2] Errores del administrador	B	B	M	M	M
	[E.19] Fugas de información	A			M	M
[test] datos de prueba	[E.18] Destrucción de información	B	M			M
	[A.15] Modificación deliberada de la información	M		M		M
	[A.6] Abuso de privilegios de acceso	MB	B	B	B	B

4.2.3. Determinación de los controles y su eficacia

Para reducir los riesgos tecnológicos encontrados en la caracterización de amenazas, es necesario definir contramedidas que impidan o disminuyan la materialización de una amenaza.

De acuerdo a lo anterior, es imprescindible contar con salvaguardas debido a que la tecnología avanza con el transcurrir del tiempo y nuevos activos aparecen conforme a este avance, dando lugar a nuevas formas de ataques para materializar una amenaza, evolucionando cada aspecto a tener en cuenta.

Para lograr el proceso de actualización de protección de activos, Magerit brinda un catálogo de salvaguardas como se muestra a continuación, con los cuales se construyen los respectivos controles que apliquen para cada activo de acuerdo con su clasificación:

- Protecciones generales u horizontales
- Protección de los datos / información.
- Protección de las claves criptográficas.
- Protección de los servicios.
- Protección de las aplicaciones (Software).
- Protección de los equipos (Hardware).
- Protección de las comunicaciones.
- Protección de los soportes de información.
- Protección de los elementos auxiliares
- Seguridad física – Protección de las instalaciones.
- Salvaguardas relativas al personal
- Salvaguardas de tipo organizativo.

Caracterización de las salvaguardas:

Cada salvaguarda está caracterizado por la eficiencia y la eficacia que posee frente a los riesgos que se quieren mitigar; donde está definido por la siguiente tabla:

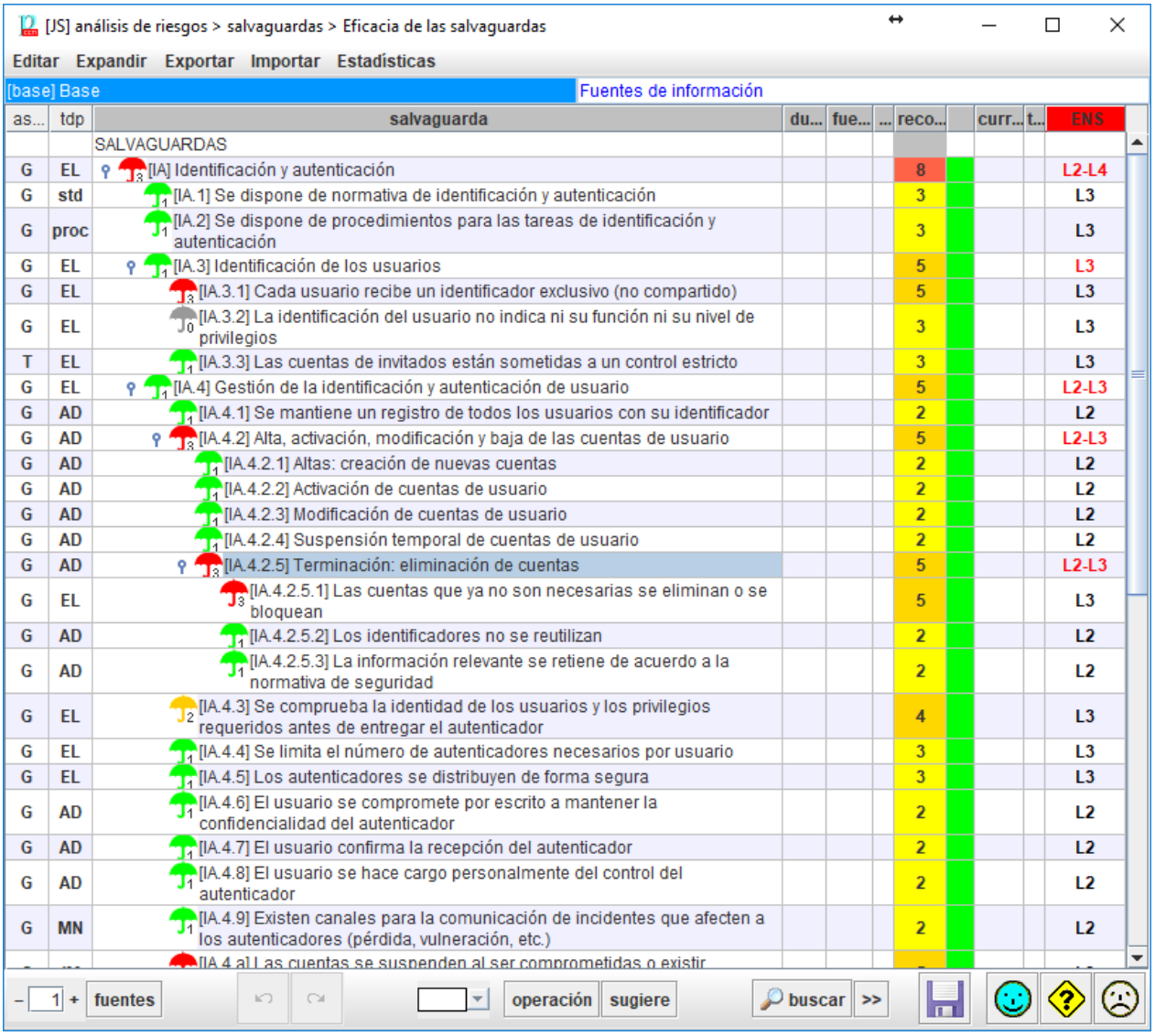
Tabla 40 Valorización de la salvaguarda

Eficacia	Nivel	Madurez
0%	L0	Inexistente
10%	L1	Inicial / ad hoc
40%	L2	reproducible, pero intuitivo
70%	L3	proceso definido
90%	L4	gestionado y medible
100%	L5	Optimizado

Valoración de los controles existentes

Mediante la herramienta PILAR la cual esta enfocada a la metodología Magerit, se realizo el ingreso de los activos a medir, asi mismo las amenazas propuestas para cada activo, que permitió que la herramienta visualizara los controles correspondientes a las amenazas y activos, asi mismo la valoración de los mismos, para realizar una mejor implementación.

Ilustración 41 Tabla de valoración de controles Magerit



as...	tdp	salvaguarda	du...	fue...	...	reco...	curr...	t...	ENS
		SALVAGUARDAS							
G	EL	[IA] Identificación y autenticación				8			L2-L4
G	std	[IA.1] Se dispone de normativa de identificación y autenticación				3			L3
G	proc	[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación				3			L3
G	EL	[IA.3] Identificación de los usuarios				5			L3
G	EL	[IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)				5			L3
G	EL	[IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios				3			L3
T	EL	[IA.3.3] Las cuentas de invitados están sometidas a un control estricto				3			L3
G	EL	[IA.4] Gestión de la identificación y autenticación de usuario				5			L2-L3
G	AD	[IA.4.1] Se mantiene un registro de todos los usuarios con su identificador				2			L2
G	AD	[IA.4.2] Alta, activación, modificación y baja de las cuentas de usuario				5			L2-L3
G	AD	[IA.4.2.1] Altas: creación de nuevas cuentas				2			L2
G	AD	[IA.4.2.2] Activación de cuentas de usuario				2			L2
G	AD	[IA.4.2.3] Modificación de cuentas de usuario				2			L2
G	AD	[IA.4.2.4] Suspensión temporal de cuentas de usuario				2			L2
G	AD	[IA.4.2.5] Terminación: eliminación de cuentas				5			L2-L3
G	EL	[IA.4.2.5.1] Las cuentas que ya no son necesarias se eliminan o se bloquean				5			L3
G	AD	[IA.4.2.5.2] Los identificadores no se reutilizan				2			L2
G	AD	[IA.4.2.5.3] La información relevante se retiene de acuerdo a la normativa de seguridad				2			L2
G	EL	[IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador				4			L3
G	EL	[IA.4.4] Se limita el número de autenticadores necesarios por usuario				3			L3
G	EL	[IA.4.5] Los autenticadores se distribuyen de forma segura				3			L3
G	AD	[IA.4.6] El usuario se compromete por escrito a mantener la confidencialidad del autenticador				2			L2
G	AD	[IA.4.7] El usuario confirma la recepción del autenticador				2			L2
G	AD	[IA.4.8] El usuario se hace cargo personalmente del control del autenticador				2			L2
G	MN	[IA.4.9] Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)				2			L2

4.2.4. Estimación del estado del riesgo

Estimación del Impacto y Riesgo Residual

Para continuar con el proceso de evaluación del riesgo y los impactos que pueden generar las amenazas encontradas con respecto a los activos evaluados, se procede a generar un análisis de las pérdidas que se presentan ya sean en la parte tecnológica o en la parte organizacional de la empresa Javesalud.

Para dar ejecución al proceso, se analizarán los siguientes dos subprocesos:

Impacto Potencial:

El impacto potencial es una medida del daño causado por una amenaza que se materializa sobre un activo. Para obtener el respectivo cálculo, se procede a tomar los valores que posee la degradación en cada una de sus dimensiones y los valores del activo en el cual se materializó la amenaza.

Ilustración 42 Parámetros de impacto

Fuente Herramienta PILAR

Ilustración 43 Impacto por activos

[JS] impacto y riesgo > impacto acumulado

potencial | current | target | ENS

activo	[D]	[I]	[C]
ACTIVOS	[A]	[A]	[A]
[E] Equipamiento	[A]	[A]	[A]
[D] Datos / Información	[B]	[A-]	[A-]
[D_Ficheros] Ficheros	[0]	[M]	[A-]
[D_backup] Copias de respaldo	[0]	[B+]	[M-]
[D_Password] Password	[0]	[M]	[A-]
[D_log] registro de actividad	[B]	[A-]	[A-]
[D_test] Datos de prueba	[B]	[M]	[0]
[SW] Aplicaciones	[A]	[A]	[A]
[SW_Browser] Navegador web	[M]	[A]	[B]
[SW_app] Servidor de aplicaciones	[M+]	[M+]	[A]
[SW_email_client] Cliente de correo electronico	[M]	[A]	[A]
[SW_Ofimatica]	[M]	[M]	[A]
[SW_av] Antivirus	[A]	[A]	[M]
[SW_os] Sistema Operativo	[A]	[A]	[M]
[SW_Backup] Sistema de Backups	[M]	[M+]	[A]

Fuente Herramienta PILAR

Nota: Tabla de impacto por amenazas ver ANEXO D y E

Riesgo Potencial:

El riesgo potencial es la medida probable del daño que puede existir sobre un sistema. Para realizar el respectivo cálculo del riesgo, es necesario conocer con anterioridad el impacto que puede generar la materialización de una amenaza sobre un activo y la probabilidad de ocurrencia de este sobre el activo analizado.

Ilustración 44 Ilustración 42 Parámetros de riesgo

Fuente Herramienta PILAR

Ilustración 45 Ilustración 43 Riesgo por activos

[JS] impacto y riesgo > riesgo acumulado

potencial | current | target | ENS

activo	[D]	[I]	[C]
ACTIVOS	{5,1}	{6,3}	{6,3}
[E] Equipamiento	{5,1}	{6,3}	{6,3}
[D] Datos / Información	{2,4}	{6,3}	{6,3}
[D_Ficheros] Ficheros	{0,93}	{5,1}	{6,3}
[D_backup] Copias de respaldo	{0,93}	{3,9}	{4,5}
[D_Password] Password	{0,93}	{5,1}	{6,3}
[D_log] registro de actividad	{2,4}	{6,3}	{6,3}
[D_test] Datos de prueba	{2,4}	{5,1}	{2,8}
[SW] Aplicaciones	{5,1}	{5,1}	{5,1}
[SW_Browser] Navegador web	{3,3}	{5,1}	{1,5}
[SW_app] Servidor de aplicaciones	{3,9}	{3,9}	{5,1}
[SW_email_client] Cliente de correo electronico	{3,3}	{5,1}	{5,1}
[SW_Ofimatica]	{3,3}	{3,3}	{5,1}
[SW_av] Antivirus	{5,1}	{5,1}	{3,3}
[SW_os] Sistema Operativo	{5,1}	{5,1}	{3,3}
[SW_Backup] Sistema de Backups	{3,3}	{3,9}	{5,1}

Fuente Herramienta PILAR

4.3. Gestión del riesgo (P3)

Teniendo en cuenta el análisis de riesgos realizado en el anterior ítem, donde se evidencian hallazgos en cuanto al impacto y a los diferentes riesgos a los que se encuentra expuesta la IPS de Javesalud, se hace necesario continuar con una calificación y clasificación de los riesgos mas significativos. Permitiendo la priorización de dichos riesgos y así asignar controles a los activos con mayor índice de riesgo.

Con finalidad de dar continuidad al proceso de toma de decisiones para asignar controles a los activos lógicos con riesgos de mayor criticidad, se procede a generar una matriz que contenga la identificación de la criticidad del riesgo en cuanto a sus dimensiones de disponibilidad, integridad y confidencialidad, haciendo relación a las amenazas encontradas anteriormente.

4.3.1. Evaluación

Ilustración 46 Evaluación de riesgos [D]

CRITICIDAD DEL RIESGO [D]				
[ACTIVO]	[AMENAZA]	[D]	[I]	[C]
[files] ficheros	[A.5] Suplantación de la identidad del usuario		M	M
	[A.6] Abuso de privilegios de acceso	M	A	A
	[A.11] Acceso no autorizado		M	A
[backup] copias de respaldo	[A.5] Suplantación de la identidad del usuario		MA	MA
	[A.6] Abuso de privilegios de acceso	M	A	M
	[A.11] Acceso no autorizado		MA	MA

[password] credenciales (ej. contraseñas)	[A.5] Suplantación de la identidad del usuario		M	M
	[A.6] Abuso de privilegios de acceso	B	MA	A
	[A.11] Acceso no autorizado		A	A
[log] registro de actividad (2)	[A.5] Suplantación de la identidad del usuario		B	
	[A.6] Abuso de privilegios de acceso		M	M
	[A.11] Acceso no autorizado	M	M	A
[test] datos de prueba	[E.15] Alteración accidental de la información	A	M	M
	[A.6] Abuso de privilegios de acceso		A	B
	[A.11] Acceso no autorizado	A	M	M

Ilustración 47 Evaluación de riesgos [SW]

CRITICIDAD DEL RIESGO [SW]				
[ACTIVO]	[AMENAZA]	[D]	[I]	[C]
[browser_Js] navegador web	[I.5] Avería de origen físico o lógico.	M		
	[A.8] Difusión de software dañino	A	MA	A
	[A.22] Manipulación de programas	M	M	B
[app_Js] servidor de aplicaciones	[I.5] Avería de origen físico o lógico.	A		
	[A.8] Difusión de software dañino	M	M	M
	[A.22] Manipulación de programas	M	B	A
	[I.5] Avería de origen físico o lógico.	A		

[email_client_Js] cliente de correo electrónico	[A.8] Difusión de software dañino	B	M	M
	[A.22] Manipulación de programas	A	A	A
	[I.5] Avería de origen físico o lógico.	M		
[oficce_Js] Ofimática.	[A.8] Difusión de software dañino	M	M	A
	[A.22] Manipulación de programas	A	A	B
	[I.5] Avería de origen físico o lógico.	A		
[av_Js] Antivirus	[A.8] Difusión de software dañino	A	A	M
	[A.22] Manipulación de programas	M	A	M
	[I.5] Avería de origen físico o lógico.	A		
[os_Js] sistema operativo	[A.8] Difusión de software dañino	M	M	A
	[A.22] Manipulación de programas	A	B	B
	[I.5] Avería de origen físico o lógico.	M		
[S_backup_Js] sistema de backup	[A.8] Difusión de software dañino	M	M	A
	[A.22] Manipulación de programas	M	MA	A

4.3.2. Tratamiento

Ilustración 48 Tratamiento de riesgos [D]

CONTROLES [D]		
[ACTIVO]	[AMENAZA]	[CONTROLES]
[files] ficheros	[E.18] Destrucción de información [E.19] Fugas de información	1. Creación de un sistema de acceso restringido para el ingreso a los respectivos ficheros que posee la empresa.

[backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	2. Implementación de un sistema de backups a los archivos involucrados, para evitar fuga de información.
	[E.15] Alteración accidental de la información	1. Verificación de las copias de respaldo en un ambiente de desarrollo.
	[E.19] Fugas de información	2. Creación de política de roles, definiendo quien será el encargado de ejecutar la copia de respaldo.
[log] registro de actividad (2)	[E.15] Alteración accidental de la información	1. Creación de política de roles, indicando el personal encargado para realizar la respectiva revisión y edición de logs.
	[A.11] Acceso no autorizado	2. Copia de respaldo de archivo de registro de actividad, para evitar una alteración accidental del log
[test] datos de prueba	[E.19] Fugas de información [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso	1. Restrincción del acceso al ambiente de pruebas por política de roles. 2. Implementación de política que solicite un doble factor de autenticación para realizar el ingreso

Ilustración 49 Tratamiento de riesgos [SW]

CONTROLES [SW]		
[ACTIVO]	[AMENAZA]	[CONTROLES]

[browser_Js] navegador web	[I.5] Avería de origen físico o lógico.	1. Mantenimiento y pruebas de navegación por medio navegador web. 2. Verificación de versión del navegador.
[app_Js] servidor de aplicaciones	[I.5] Avería de origen físico o lógico. [E.21] Errores de mantenimiento / actualización de programas (software)	1. Plan estructurado de mantenimiento y actualización del servidor de aplicaciones. 2. Servidores de aplicaciones de respaldo
[oficce_Js] Ofimática.	[I.5] Avería de origen físico o lógico. [A.22] Manipulación de programas [E.21] Errores de mantenimiento / actualización de programas (software)	1. Validaciones de compilación y actualizaciones del software. 2. Generación de registro personalizado para activación de licencia
[av_Js] Antivirus	[A.8] Difusión de software dañino	1. Plan estructurado de mantenimiento y actualización del antivirus. 2. Generación de alertas de software malicioso.
[os_Js] sistema operativo	[I.5] Avería de origen físico o lógico. [E.21] Errores de mantenimiento /	1. Creación de plan de capacitación de auxiliares de tecnología para evitar errores en mantenimiento.

	actualización de programas (software) [A.22] Manipulación de programas [E.21] Errores de mantenimiento / actualización de programas (software)	2. Implementación de sistema de monitoreo para el S.O
[S_backup_Js] sistema de backup	[A.8] Difusión de software dañino [A.22] Manipulación de programas	1. Capacitación del personal encargado de sacar las copias de respaldo. 2. Sistema de tercerización de procesos de backups para transferir el riesgo.

4.3.3. Políticas de seguridad

Con el objeto de mejorar el nivel de seguridad de la información de Javesalud, se definen las siguientes políticas:

Información

Política de clasificación de la información de las bases de datos utilizadas por la entidad, con el fin de garantizar la disponibilidad, integridad y confidencialidad de los registros

Recurso Humano

Política de responsabilidad y capacitación en el proceso de incorporación de personal nuevo

Política de confidencialidad de datos por parte del personal de la entidad

Política de comunicación de necesidades y requerimientos del personal

Política de bitácoras y registro de novedades en información

Política de capacitación de actualizaciones y mantenimiento a los colaboradores del área de tecnología

Accesos

Política de entrega de elementos archivos y funciones de colaboradores desvinculados a la entidad

Política de verificación de roles en cambio de departamento o funciones de los colaboradores de la entidad

Política de cambio de contraseñas en herramientas y sistemas utilizados por colaboradores desvinculados de la entidad.

Política de asignación de usuarios personalizados a todos los colaboradores de la entidad que tengan acceso a las herramientas de la entidad.

Política de acceso a información de dependencias diferentes a la presente del colaborador mediante solicitud de autorización escrita.

Política de verificación de usuarios redundantes en el directorio activo

Política de cambio obligatorio de contraseñas con cierto intervalo de tiempos.

Política de restablecimiento de contraseña olvidada

Política de estructura de contraseñas seguras

Seguridad física y del entorno

Política de almacenamiento de backup en lugar diferente al del procesamiento de la información

Comunicaciones y operaciones

Plan de contingencias y plan de recuperación en caída de sistema

Política de restricción de software no autorizado por la gerencia de tecnología.

Política de actualización y escaneo periódico de antivirus.

Política de procedimientos básicos para los colaboradores con el fin de detectar software malicioso

Política de simulacro de caída de sistema.

5. Conclusiones

La Empresa Javesalud IPS, no cuenta con un proceso de gestión de riesgos informáticos para garantizar la seguridad informática del sistema, por lo cual el presente trabajo apoyará el respectivo proceso de mitigación de riesgos a nivel lógico de activos de información que se encuentran en la organización.

Fue posible encontrar y enlistar los activos lógicos que posee la empresa Javesalud, donde se detectaron las amenazas relacionadas a cada activo y el impacto que este generaría en caso de materializarse. Al igual que los controles necesarios a implementar para reducir el riesgo de perdida de información, que puede reflejarse desde el ingreso de cualquier personal sin restricción a los ficheros, hasta un backup mal ejecutado por personal sin experiencia ni capacitación.

Al momento de realizar la clasificación de los activos de acuerdo a su criticidad, se encontró que la empresa posee debilidades en cuanto a la manipulación de estos activos, donde se refleja la falta de gestión de políticas de seguridad de la información, debido a que la mayor parte de los colaboradores de la entidad conocen los procedimientos básicos de seguridad, sin embargo, no existe un proceso estructurado documentado.

A través de una fórmula de muestro probabilístico simple se identifico una muestra de colaboradores, al cual se implementó una encuesta sobre el conocimiento que se poseía del aseguramiento de información y respaldo de documentación digital; a lo que se evidenció la falta de implantación de un manual de políticas de seguridad informática, que permitiera gestionar los procesos de utilización de dichos activos lógicos.

6. Productos que entregar

El proyecto será realizado en el ámbito de la seguridad lógica de la información en la entidad, con el fin de generar una visión de los riesgos y las vulnerabilidades que posee la infraestructura que salvaguarda la información de los usuarios con finalidad de generar propuestas concretas de cómo mitigar dichos riesgos y vulnerabilidades encontradas, los entregables son:

- Un informe del estado actual de los activos lógicos de la entidad encaminado a la validación de un estado inicial, y su importancia en la entidad.
- Una matriz de riegos realizado a partir de las metodologías de análisis de riesgos determinadas que permita una visualización general de la vulnerabilidad de los activos inventariados
- Un mapa de calor o la herramienta que el modelo determinado para tal fin, que nos permita determinar la criticidad de los riesgos, tomando como variables su impacto y frecuencia.

Un plan de mitigación de riesgos, documentando los controles y las buenas prácticas recopiladas, que puedan permitir a la alta gerencia una toma de decisiones más adecuada a la hora de proteger los activos lógicos de la entidad.

7. Resultados esperados e impactos

AL finalizar el proyecto se debe poder realizar la identificación de los riesgos y vulnerabilidades de JAVESALUD IPS, la observación de e identificación de los riesgos de mayor impacto a través de las matrices correspondientes, y un informe donde se podrá realizar la validación de los posibles procesos, protocolos y tareas que permitan mitigar los riesgos de mayor impacto en la entidad, a través de la generación de un informe con las propuestas generadas para la mitigación de los riesgos y vulnerabilidades encontradas en JAVESALUD IPS, superando así la problemática de estar expuestos a riesgos y vulnerabilidades de activos lógicos.

8. Estrategias de comunicación

En las estrategias de comunicación se realizará los modelos que exige el proyecto de grado adicional los procesos de los resultados deberán socializarse con el personal de la entidad para asimilar las tareas propuestas para la mitigación de los riesgos y vulnerabilidades, en ese orden se realizara el poster del proyecto, el artículo, la entrega del proyecto final y por supuesto un plan de socialización de los empleados involucrados en el proceso de seguridad de la información.

9. Bibliografía

- Michael Jeremey, (septiembre 2011), Recuperado de: http://kidshealth.org/es/parents/ehrs-esp.html
- Beltrán Marta, (Mayo 2017), Conceptos de amenaza, riesgo y vulnerabilidad, Recuperado de: https://miriadax.net/web/ciberseguridad-entender-los-ataques-para-desplegar-contramedidas/reto?p_auth=DPW2bA2R&p_p_id=lmsactivitieslist_WAR_liferaylmsportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&r_p_r_p564233524_actId=1&_lmsactivitieslist_WAR_liferaylmsportlet_javax.portlet.action=goToModule&p_r_p_564233524_moduleId=58002&_lmsactivitieslist_WAR_liferaylmsportlet_themeId=1
- Pillou Jean-François, (noviembre 2013), Definición paciente, Recuperado de: http://salud.ccm.net/faq/15489-paciente-definicion
- Portal de Administración Electrónica Ministerio de Hacienda y Función Pública Secretaría General de Administración Digital, Gobierno España, (2017), MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Recuperado de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WfCYrmj9Tcc
- Markus Erb. Gestión de Riesgo en la Seguridad Informática [en línea]. https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion
- Garaycochea Virginia (marzo 2003), Auditoria Medica, Recuperado de: http://sisbib.unmsm.edu.pe/bvrevistas/paediatrica/v03_n1/auditor%C3%ADa.htm
- Fonasa, (enero 2017), Consultas médicas, Recuperado de: https://www.fonasa.cl/sites/fonasa/beneficiarios/coberturas/plan-general/consultas

- Intef (enero 2017), Aulas en red, aplicaciones y servicios. Windows, Recuperado de: http://www.ite.educacion.es/formacion/materiales/85/cd/windows/5DirectorioActivo/index.html).
- ORACLE (enero 2010), Guía del administrador de negocio de Sun Identity Manager 8.1 Recuperado de: https://docs.oracle.com/cd/E19957-01/821-0062/byaft/index.html
- COMISIÓN INTERAMERICANA DE TELECOMUNICACIONES. (2009). Gestión de riesgos de seguridad. Recuperado en: http://www.oas.org/en/citel/infocitel/2009/septiembre/seguridad_e.asp
- ISO27000.ES. (junio 2015). Recuperado de: http://www.iso27000.es/.
- INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN ISO/IEC 27001. 2013 primera actualización. Bogotá. ICONTEC
- Garavito Robles Hina Luz, (octubre 2015), análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información.
- Nelson Gómez (febrero 2011), Recomendaciones de seguridad informática, Universidad Javeriana.

ANEXO A

Encuesta Alta Gerencia

Seguridad de la información DG

¿La entidad cuenta con presupuesto para seguridad de la información?

- si
- No

¿La seguridad de la información hace parte de los temas tratados en los comités de dirección?

- si
- No

¿Conoce los riesgos de los objetivos estratégicos basados en la seguridad de la información?

- si
- No

¿La entidad tiene algún plan de controles enfocado a la seguridad de la información?

- si
- No

¿Qué dependencia está encargada de los planes seguridad de la información?

- Dirección General
- Dirección Medica
- Dirección Académica
- Dirección de Gestión Humana
- Dirección Administrativa
- Dirección de Operaciones y Calidad

ANEXO B

Encuesta Nivel Gerencial

Seguridad de la Información Direcciones

¿A qué Dirección pertenece?

- Dirección Medica
- Dirección Académica
- Dirección Gestión Humana
- Dirección Administrativa
- Dirección Operaciones y Calidad

¿Tiene la Dirección procesos de controles en todos sus procesos?

- Si
- No

¿Tiene el inventario de todos los archivos que se manejan en los procesos del macroproceso?

- Si
- No

¿Posee manuales de manejo de los sistemas de información de la entidad?

- Si
- No

¿que herramientas utilizan para los procesos de la entidad?

- Solo Sistemas de información
- Solo Documentación física
- Solo Ofimática (word, excel, power point)
- Todas las anteriores

¿Dónde es el almacenamiento principal de los documentos y procesos de la Dirección?

- Equipos Locales
- Servidor externo
- Servidor interno
- Nube
- Todas las anteriores
- No sabe

ANEXO C

Encuesta Nivel Operativo

¿Si le envían un mensaje a su correo personal de su banco de confianza para que ingrese a un link especifico que le solicita información confidencial, usted que hace?

- Utiliza el Link sugerido por el banco e ingresa sus datos personales
- Llama a servicio al cliente del banco para confirmar el correo recibido
- Elimina el correo
- Solicita ayuda de un amigo
- Llama a soporte de la oficina de Tecnología

¿A su correo institucional han llegado correos masivos de remitentes externos a la entidad?

- Si
- No

¿Si al navegar en Internet aparece una ventana y le pide dar aceptar o descargar?

usted le da clic sin preocuparse de que se trata

- Lee con detenimiento el mensaje que aparece
- Pide ayuda de alguien cercano que sepa de sistemas o llama a la oficina de tecnología
- Le da cancelar o cerrar a la ventana

¿Usted cierra la sesión de su sistema cada vez que se levanta de su equipo?

- Si
- No

¿Cómo define sus contraseñas?

- Utiliza los nombres de sus padres o de sus hijos para que sea más fácil de recordar
- Utiliza como mínimo 8 caracteres, que contenga letras, números y símbolos

- Utiliza una palabra corta acompañada de un número
- Utiliza una frase corta fácil de recordar

¿En su memoria USB, en su celular u otro dispositivo portable acostumbra a llevar copias de la información de la Oficina?

- Nunca
- Algunas veces
- Con frecuencia
- Siempre

¿Si a Usted le solicitan conservar la información a través de medios que garanticen su preservación, en otras palabras hacer copias de seguridad de la información gestionada en la entidad, prefiere?

- No darle importancia
- Conservarla en su computador
- Conservarla en los discos de red o carpetas compartidas alojadas en otro computador a fin de preservarla
- Guardarla en otros medios (Celular, CD, USB, Discos externos)

¿Si crea copias de seguridad de la información de la entidad en medios físicos como DVD, CD, USB, donde las ubica?

- En el cajón de su oficina
- en un archivo especial destinado para ello
- en su casa

¿Si a Usted le asignan una contraseña, para evitar olvidarla acostumbra?

- Registrarla en un archivo

- Copiarla en una hoja que deja encima del escritorio
- Copiarla en un Post-it y lo pega en la pantalla del computador
- Memorizarla
- Revelarla a un tercero

¿Usted hace parte del equipo de la entidad que está evaluando un dato que va a ser publicado próximamente, al subir al ascensor para salir a almorzar se encuentra un amigo de otra dependencia en el ascensor al cual le comenta el información de la dato, usted no se fija que en el ascensor iba un periodista carnetizado del diario El Tiempo días después aparece la noticia antes que la publique la entidad, usted que hace?

- Llama al diario El Tiempo a quejarse
- Admite el error cometido y lo comenta con sus superiores
- Pregunta al señor vigilante del edificio si conoce al tipo
- Ninguna de las anteriores

¿Usted cree que la información personal de los empleados de la entidad tales como: Dirección casa, teléfonos, la conocen?

- Todos los empleados de la entidad
- Los administradores del sistema de Recursos Humanos
- Usted solamente
- Ninguna de las anteriores

¿Si Usted está buscando información en un directorio o carpeta privada, e involuntariamente se da cuenta que puede ingresar a la(s) carpeta(s) de otra(s) dependencia(s), que acción toma?

- Navega por las subcarpetas y revisa la información existente
- No le da importancia y continúa con su búsqueda

- Comenta con otro(a) compañero (a) la situación
- Notifica a sistemas este hallazgo

¿Cuál de las siguientes opciones considera adecuada para él envió de impresiones a la impresora de su dependencia?

- Se puede imprimir cualquier tipo de documento
- Solo se deben imprimir documentos institucionales
- Se puede imprimir cualquier cosa pero sin que se den cuenta
- No se puede imprimir nada porque desde la Oficina de Informática nos vigilan
- La oficina de tecnología no vigila las impresiones y por esta razón se puede imprimir cualquier cosa

¿Si al ingresar en alguna página de Internet, y esta se ve correctamente, y le sale el siguiente aviso “para poder ver la página correctamente debe instalar un controlador X”, ¿usted realiza alguna de las siguientes acciones?

- Permite la Instalación
- Investiga para qué sirve el controlador que se requiere instalar
- Llama a Soporte para que le indique que acción realizar
- Acepta que no puede instalarlo, porque por seguridad están restringidas las descargas

¿Si una entidad externa solicitan a una Dependencia de la organización información perteneciente a la organización, usted como funcionario que haría?

- Le dice que le envía la información por correo electrónico
- Le dice que venga a la oficina y le entrega una copia
- Consulta el directorio de fuentes de información para saber quién es el responsable
- Consulta con jefe inmediato si está permitido compartir esta información

¿Usted mantiene la información de naturaleza confidencial de la entidad en:

- La carpetas Mis documentos de su área
- La carpeta Escritorio de su Área
- Una carpeta ubicada en la raíz disco C
- En una carpeta ubicada en la raíz de otra unidad (si esta se encuentra disponible)

¿Siempre que coloca su unidad USB en su computador UD?

- Le pasa el antivirus, antes de acceder a ella
- No le pasa en antivirus, y realiza intercambios de información

¿Si alguno de sus conocidos le informa que le están llegando mensajes raros desde su cuenta de correo institucional usted:

- Llamar a la mesa de ayuda e informar de la situación
- No reporta y cambia la clave de su sesión, pensando que con esto solucionará el problema
- No le da importancia al comentario

¿Usted acostumbra a usar correos diferentes a los institucionales para envió de información que tiene que ver con la entidad?

- Si
- No

¿Acostumbra a ir a cafés Internet a consultar su cuenta de correo institucional o de la entidad donde trabaja?

- Si
- No

¿Considera que la información de propiedad de la entidad debe ser privada e intransferible, por tal razón se debe:

- Mejorar los controles de acceso
- Impedir el uso de dispositivos externos que permitan la difusión de la información
- Capacitar a los usuarios en el buen manejo de la información de propiedad de la entidad
- Otra

ANEXO D

Ilustración 50 Tabla de Impacto por amenazas [D]

IMPACTO [D]				
[ACTIVO]	[AMENAZA]	[D]	[I]	[C]
[files] ficheros	[E.15] Alteración accidental de la información		[B]	
	[E.18] Destrucción de información	[0]		
	[E.19] Fugas de información			[M]
	[A.5] Suplantación de la identidad del usuario		[M]	[A-]
	[A.6] Abuso de privilegios de acceso	[0]	[M]	[A-]
	[A.11] Acceso no autorizado		[M]	[A-]
[backup] copias de respaldo	[E.15] Alteración accidental de la información		[0]	
	[E.18] Destrucción de información	[0]		
	[E.19] Fugas de información			[B]
	[A.5] Suplantación de la identidad del usuario		[B+]	[M-]
	[A.6] Abuso de privilegios de acceso	[0]	[B+]	[M-]
	[A.11] Acceso no autorizado		[B+]	[M-]
[password] credenciales (ej. contraseñas)	[E.15] Alteración accidental de la información		[B]	
	[E.18] Destrucción de información	[0]		
	[E.19] Fugas de información			[M]
	[A.5] Suplantación de la identidad del usuario		[M]	[A-]
	[A.6] Abuso de privilegios de acceso	[0]	[M]	[A-]
	[A.11] Acceso no autorizado		[M]	[A-]
	[E.15] Alteración accidental de la información		[B]	

	[E.18] Destrucción de información		[B]	
	[E.19] Fugas de información	[B]		
[log] registro de actividad (2)	[A.5] Suplantación de la identidad del usuario		[A-]	
	[A.6] Abuso de privilegios de acceso		[M]	[A-]
	[A.11] Acceso no autorizado	[B]	[M]	[A-]
	[E.15] Alteración accidental de la información	[B]	[M]	[0]
	[E.18] Destrucción de información		[B]	
[test] datos de	[E.19] Fugas de información	[B]		
prueba	[A.5] Suplantación de la identidad del usuario			[0]
	[A.6] Abuso de privilegios de acceso		[M]	[0]
	[A.11] Acceso no autorizado	[B]	[M]	[0]

ANEXO E

Ilustración 51 Tabla de Impacto por amenazas [SW]

IMPACTO [SW]				
[ACTIVO]	[AMENAZA]	[D]	[I]	[C]
[browser_Js] navegador web	[I.5] Avería de origen físico o lógico.	[M-]		
	[E.8] Difusión de software dañino	[B]	[M]	[0]
	[E.20] Vulnerabilidades de los programas (software)	[0]	[M+]	[0]
	[E.21] Errores de mantenimiento / actualización de programas (software)	[0]	[B]	
	[A.8] Difusión de software dañino	[M]	[A]	[B]
	[A.22] Manipulación de programas	[M-]	[A]	[B]
[app_Js] servidor de aplicaciones	[I.5] Avería de origen físico o lógico.	[M]		
	[E.8] Difusión de software dañino	[B+]	[B+]	[M]
	[E.20] Vulnerabilidades de los programas (software)	[0]	[M-]	[M+]
	[E.21] Errores de mantenimiento / actualización de programas (software)	[0]	[0]	
	[A.8] Difusión de software dañino	[M+]	[M+]	[A]
	[A.22] Manipulación de programas	[M]	[M+]	[A]
	[I.5] Avería de origen físico o lógico.	[M-]		
	[E.8] Difusión de software dañino	[B]	[M]	[M]

[email_client_Js] cliente de correo electrónico	[E.20] Vulnerabilidades de los programas (software)	[0]	[M+]	[M+]
	[E.21] Errores de mantenimiento / actualización de programas (software)	[0]	[B]	
	[A.8] Difusión de software dañino	[M]	[A]	[A]
	[A.22] Manipulación de programas	[M-]	[A]	[A]
	[I.5] Avería de origen físico o lógico.	[M-]		
	[E.8] Difusión de software dañino	[B]	[B]	[M]
[oficce_Js] Ofimática.	[E.20] Vulnerabilidades de los programas (software)	[0]	[B+]	[M+]
	[E.21] Errores de mantenimiento / actualización de programas (software)	[0]	[0]	
	[A.8] Difusión de software dañino	[M]	[M]	[A]
	[A.22] Manipulación de programas	[M-]	[M]	[A]
	[I.5] Avería de origen físico o lógico.	[A-]		
	[E.8] Difusión de software dañino	[M]	[M]	[B]
[av_Js] Antivirus	[E.20] Vulnerabilidades de los programas (software)	[B]	[M+]	[B+]
	[E.21] Errores de mantenimiento / actualización de programas (software)	[B]	[B]	
	[A.8] Difusión de software dañino	[A]	[A]	[M]
	[A.22] Manipulación de programas	[A-]	[A]	[M]

	[I.5] Avería de origen físico o lógico.	[A-]		
	[E.8] Difusión de software dañino	[M]	[M]	[B]
	[E.20] Vulnerabilidades de los programas (software)	[B]	[M+]	[B+]
[os_Js] sistema operativo	[E.21] Errores de mantenimiento / actualización de programas (software)	[B]	[B]	
	[A.8] Difusión de software dañino	[A]	[A]	[M]
	[A.22] Manipulación de programas	[A-]	[A]	[M]
	[I.5] Avería de origen físico o lógico.	[M-]		
	[E.8] Difusión de software dañino	[B]	[B+]	[M]
	[E.20] Vulnerabilidades de los programas (software)	[0]	[M-]	[M+]
[S_backup_Js] sistema de backup	[E.21] Errores de mantenimiento / actualización de programas (software)	[0]	[0]	
	[A.8] Difusión de software dañino	[M]	[M+]	[A]
	[A.22] Manipulación de programas	[M-]	[M+]	[A]

ANEXO F

Normas, recomendaciones y buenas prácticas

Contraseñas o *passwords*

Las siguientes normas y requisitos que deben cumplir las contraseñas cada vez que se asigne o se realice el cambio:

- Su longitud debe ser mínimo de ocho (8) caracteres
- Estar compuestas por caracteres alfanuméricos (números y letras). Se recomienda una letra mayúscula, un número. Las contraseñas que utilizan letras y números son más difíciles de adivinar.
- No podrán reusarse ninguna de las ultimas 3 contraseñas utilizadas
- Las contraseñas deberán cambiarse de forma obligatoria cada 30 días.
- Las contraseñas no deben contener el nombre de cuenta del usuario o de su nombre completo, ya sea de forma parcial o completa.
- No escriba las contraseñas en ningún medio, ni las revele por vía telefónica, correo electrónico ni por ningún otro medio.
- No comparta su contraseña. Las contraseñas son de uso personal y por ningún motivo "las preste" a otros usuarios. En ningún caso los administradores de las cuentas de servicios informáticos le pedirán su contraseña.
- No digite sus claves secretas en computadores de otras personas, de sitios públicos y/o no confiables.

Correo electrónico

Tenga en cuenta que el correo electrónico a través de las redes informáticas e Internet no es seguro. Sea precavido con los mensajes de correo electrónico que envía, recibe y conserva:

- No abra archivos adjuntos al correo electrónico de personas desconocidas, sospechosas, de una fuente de poca confianza o si el asunto del mensaje es dudoso, pueden contener "virus", los cuales podrían dañar su PC.
- Borre “cadenas” de correo electrónico y correos con propaganda (*spam*) de su buzón, pueden ser fastidios u ofensivos y pueden generar riegos de seguridad y privacidad.
- Estar alerta es la mejor defensa contra los engaños “*phishing*”.
- Si llegara a recibir un correo electrónico anunciando que su cuenta de ahorro ha sido cerrada, o que es necesario que usted confirme un pedido, o que es necesario que envíe su contraseña, no responda el correo ni “de *clic*” en ninguno de los enlaces resaltados en el correo. Si usted quiere confirmar si el correo electrónico es legítimo, contacte telefónicamente o por escrito a la organización o a la persona directamente.

Internet

- Cuando use un programa de mensajería instantánea (por ejemplo: Messenger, WhatsApp, Skype), no lea mensajes ni “de *clic*” en enlaces que le envíen usuarios. La mensajería instantánea puede ser un medio para transmitir virus y otros programas maliciosos, y es otra manera para iniciar engaños “*phishing*”.
- Proceda con cautela cuando descargue archivos desde Internet. Revise que el sitio Web al que se conecta es legítimo y acreditado. Si tiene dudas es recomendable que no descargue el archivo. Si usted descarga programas (software) de Internet, sea especialmente cuidadoso con los programas que no tienen costo, los cuales frecuentemente ocultan programas no deseados…
- Por eso tenga siempre cuidado con su cuenta de usuario y contraseña. No la revele a nadie por ningún motivo, ni a través de ningún medio y siempre que las use hágalo en

computadores conocidos

- Realice siempre sus transacciones desde un computador seguro.
- No acuda a los café Internet para hacer operaciones bancarias.
- No olvide revisar sus extractos de cuenta y de tarjetas de crédito regularmente.
- Los robos de identidad permiten usar su información personal para abrir cuentas, hacer compras, y enredarle la vida.
- Por eso verifique con frecuencia el estado de sus cuentas y tarjetas.
- Si usted descubre que su información personal ha sido comprometida, alerte a los bancos de inmediato para que le bloqueen sus cuentas y tarjetas.

Información y el computador

- Recuerde siempre cerrar la aplicación cuando haya terminado. Es rápido, fácil y evita que otra persona tenga acceso a la aplicación a su nombre.
- Bloquee su computador en el momento en que se retire del puesto de trabajo. Lo podrá desbloquear con su contraseña del usuario.
- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, tenga cuidado de dejar la información confidencial protegida bajo llave. Esto incluye: CDs, DVDs, dispositivos de almacenamiento USB, entre otros.
- Realice sus actividades en lo posible solo desde el computador de oficina asignado.
- Asegúrese de que su PC tenga un buen antivirus. Revise que el software de antivirus en el computador se mantenga instalado y actualizado.
- Verifique que el sistema operativo de su computador y todos sus aplicativos (software) se encuentre actualizado en las últimas versiones a las que tenga derecho.
- Genere copias de sus archivos (back up) frecuentemente. Si un virus infecta sus archivos,

al menos podrá reemplazarlos con una copia. Una recomendación es que almacene sus copias (guardadas en CDs o memorias "USB") en un sitio físico seguro diferente al de su computador

- El uso de medios de almacenamiento removibles (USBs, CDs, DVDs, disquetes, reproductores de mp3, entre otros) y equipos personales portátiles debe realizarse con precaución. Es importante verificar que estos dispositivos se encuentren libres de virus y código malicioso, antes de utilizarlos en su computador.
- Un virus o programa malicioso pude dañar su información o pretender robarle datos personales, contraseñas o información valiosa almacenada, transmitida o tecleada en su computador.

Evite ser burlado con técnicas de ingeniería social

- Recuerde que, si algo suena demasiado bueno para ser verdad, muy probablemente lo sea.
- Pregúntese usted mismo: porque debería YO tener un tratamiento especial sobre millones de otros usuarios de internet. Si usted no encuentra una buena razón, esto probablemente es una estafa.
- No crea en todo lo que lee. Solo porque un email o un sitio web parece atractivo no significa que le esté diciendo la verdad.
- Se paciente y cuidadoso. Muchos usuarios han sido víctimas de internet debido a que no se detuvieron a pensar, y en su lugar actuaron impulsivamente y dieron *clic* en un llamativo enlace o en un adjunto que parecía interesante sin pensar en las posibles consecuencias.
- A menos que usted este seguro de la identidad de una persona o de una autoridad que le requiera información, nunca provea su información personal o información acerca de su

organización.

- No revele información personal o financiera por email. Desconfíe de los emails que le indica que siga un enlace para ingresar la información.
- Si usted cree que un email no es legítimo, intente verificarlo contactando a la compañía directamente. Pero no use la información de contacto indicada en el email, esta puede ser falsa; busque la información de contacto usted mismo.
- Verifique dos veces las URLs de los sitios web que visita. Algunos sitios web de phishing lucen idénticos a los reales, pero la URL podría ser substancialmente diferente.
- Sea cauteloso al enviar información sensitiva a través de internet si usted no confía en la seguridad del sitio web.
- Sospeche de llamadas y correos no solicitados que preguntan por información acerca de empleados de la organización y otro tipo de información. Esta puede ser una llamada de un estafador. (Gomez, febrero 2011).